User's Manual

IP7251 Network Camera

Intelligent Video Content Analysis



VIVOTEK

Table of Contents

Overview

VIVOTEK unveils its first intelligent network camera IP7251 in the line of progressive-scan series which incorporates embedded video content analysis. The intelligent detection effectively raises the sensitivity of this network camera and makes your monitoring tasks easier with correct information. Incorporating a powerful digital signal processor (DSP) dedicated to the video content analysis, it features three reliable and helpful detections including tampering detection, moving object detection, and loitering detection. With the tampering detection, it is capable of detecting incidents such as shooting redirection, blocking or defocusing of cameras, or even spray-painted. For motion detection function, it is capable of distinguishing between creature's motions and still backgrounds or natural movements like swaying trees, waves or sunset so as to prevent the false alarms from environmental noise. Additionally, a suspicious object in the predefined area (window) will trigger alarms once the dwelling time of the object is longer than the given time. By embedding the video content analysis into the network camera rather instead of back-end software platform, IP7251 greatly reduces the server workload, network bandwidth, and storage requirement. IP7251 is achieved with a powerful combination of cutting-edge features: a Sony progressive scan CCD sensor, a removable IR-cut filter, simultaneous dual streams, PoE compliant with 802.3af, 3GPP mobile surveillance, two-way audio by SIP protocol, and digital I/O.
With the intelligent detection function, VIVOTEK IP7251 can effectively prevents unwanted noise components from accidentally triggering an alarm, providing a more reliable detection method, thus reducing the number of false alarms.

Read before use

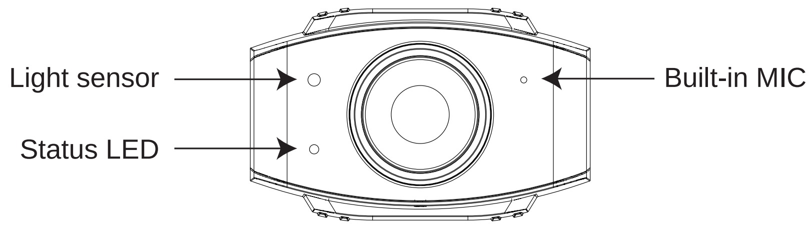
The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but also can be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.
It is important to first verify that all contents received are complete according to the Package contents listed below. Take notice of the warnings in Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damages due to faulty assembly and installation. This also ensures the product is used properly as intended.
The Network Camera is a network device and its use should be straightforward for those who have basic network knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For the creative and professional developers, the URL Commands of the Network Camera section serves to be a helpful reference to customize existing homepages or integrating with the current web server.

Package contents

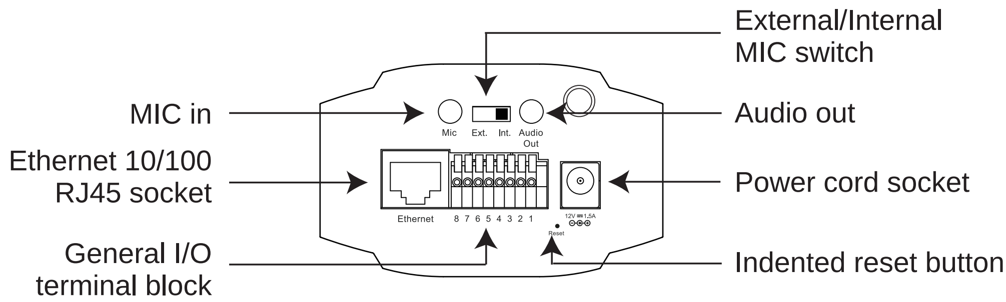
■ IP7251
■ Power adapter
■ Camera stand
■ CS-mount lens
■ Quick installation guide
■ Software CD
■ Warranty card
■ L-type hex key wrench / C-mount ring (for C-mount lens)

Physical description

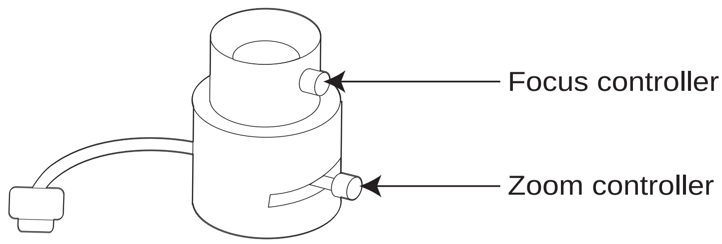
Front panel



Back panel



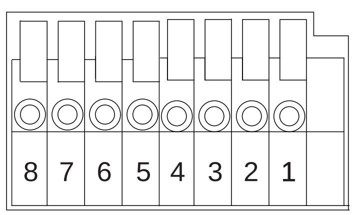
Lens



General I/O Terminal Block

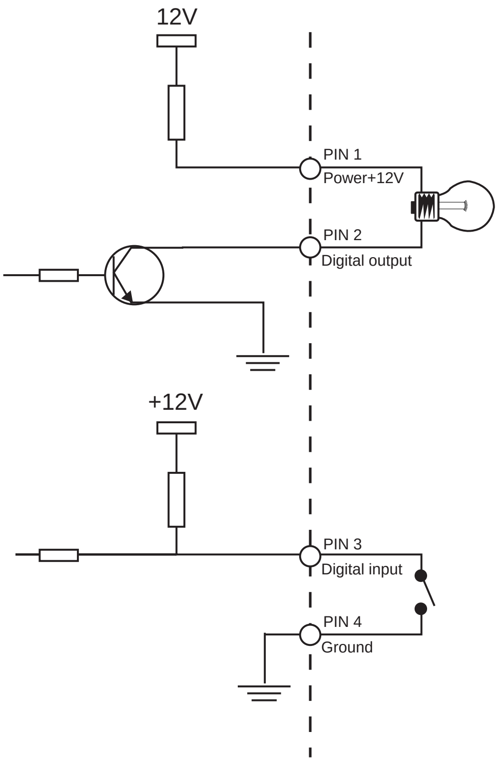
This Network Camera provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below.

Pin	Name
1	Power
2	Digital Output
3	Digital Input
4	Ground
5	AC 24V input
6	AC 24V input
7	RS-485 -
8	RS-485 +



DI/DO Diagram

Refer to the following illustration for connection method.

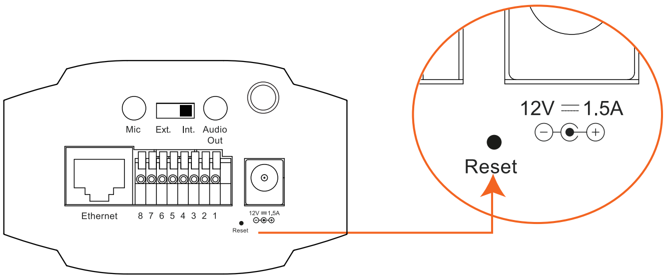


Status LED

The LED indicates the status of the Network Camera.

Status LED	Description
Blinking red (short)	1. The Network Camera is booting up. 2. Reboot or restore the Network Camera.
Steady green (long)	The Network Camera is trying to obtain an IP address.
Blinking green every other second	The network is setup (system up).
Fast blink orange	During the upgrade firmware process.

Hardware Reset



There is an indented reset button on the back panel of the Network Camera. It is used to reboot the Network Camera or restore the Network Camera to factory default. Sometimes rebooting the Network Camera could set the Network Camera back to normal state. If the problems remain after rebooted, restore the Network Camera to factory default and install again.

Reboot: Press and release the indented reset button once with a needle. The status LED will blink in red.

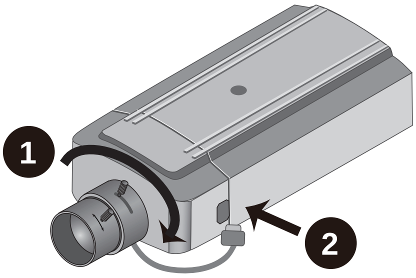
Restore: Press the indented reset button with a needle continuously for over five seconds. The status LED will blink in red. Note that all settings will be restored to factory default.

Installation

Hardware installation

Follow the steps below to mount the lens to the Network Camera:

1. Mount the lens by turning it clockwise onto the camera mount until it stops. If necessary, turn the lens counterclockwise slowly until it gets the best attitude.
2. Connect the lens cable plug to the camera connector.

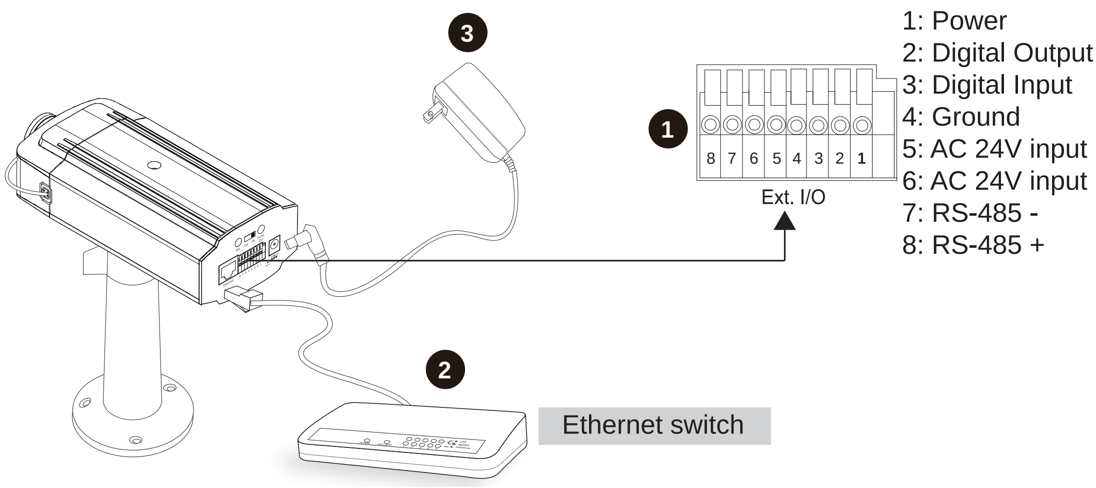


Network deployment

Setup the Network Camera over the Internet

This section explains how to configure the Network Camera to Internet connection.

1. If you have external devices such as sensors and alarms, make connection from general I/O terminal block.
2. Connect the camera to a switch via Ethernet cable.
3. Connect the supplied power cable from the camera to a power outlet.

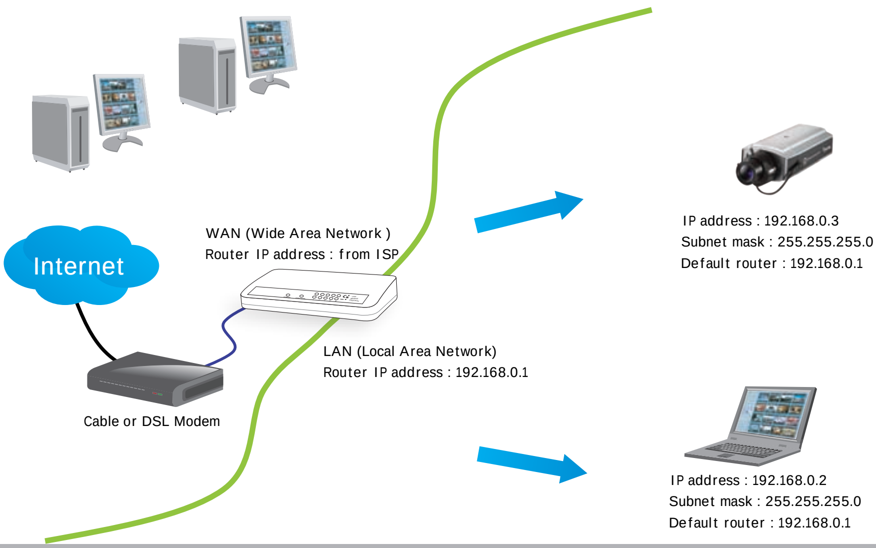


There are several ways to setup the Network Camera over the Internet. The first way is to setup the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated as below. About how to get your IP address, please refer to Software installation on page 10 for details.



2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

- HTTP port
- RTSP port
- RTP port for audio
- RTCP port for audio
- RTP port for video
- RTCP port for video

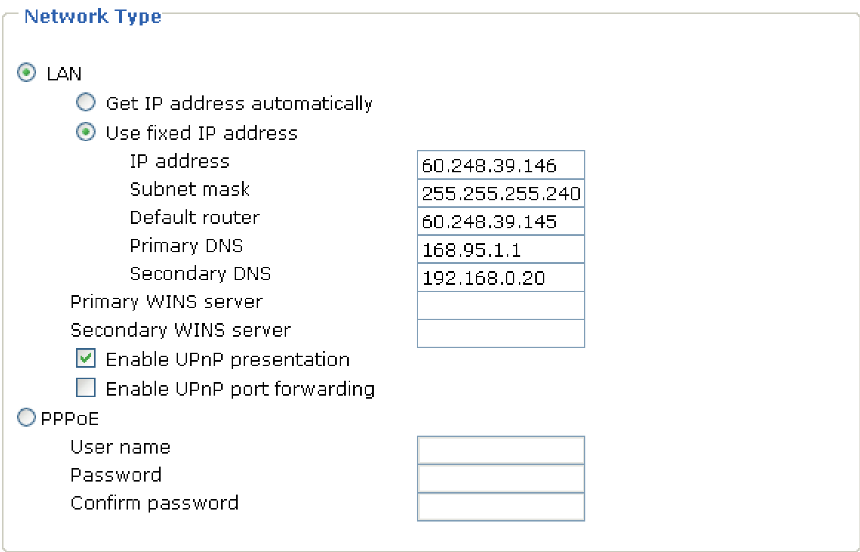
If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to the user's manual of your router.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 24 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera and follow the steps below.

1. Set up the Network Camera in a LAN. Please refer to Software installation on page 10 for details.
2. Go to Configuration > Network > Network Type. Select LAN > Use fixed IP address.
3. Enter the static IP, Subnet mask, Default router, Primary DNS provided by your ISP.



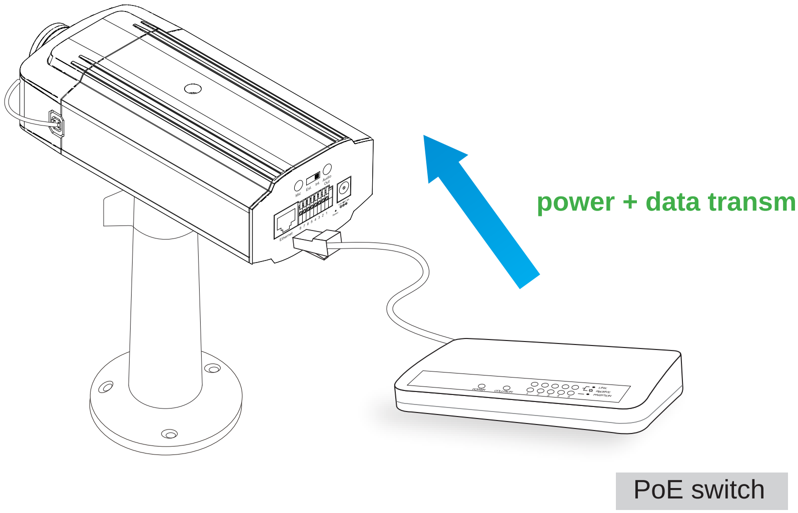
Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 25 for details.

Set up the Network Camera through Power over Ethernet (PoE)

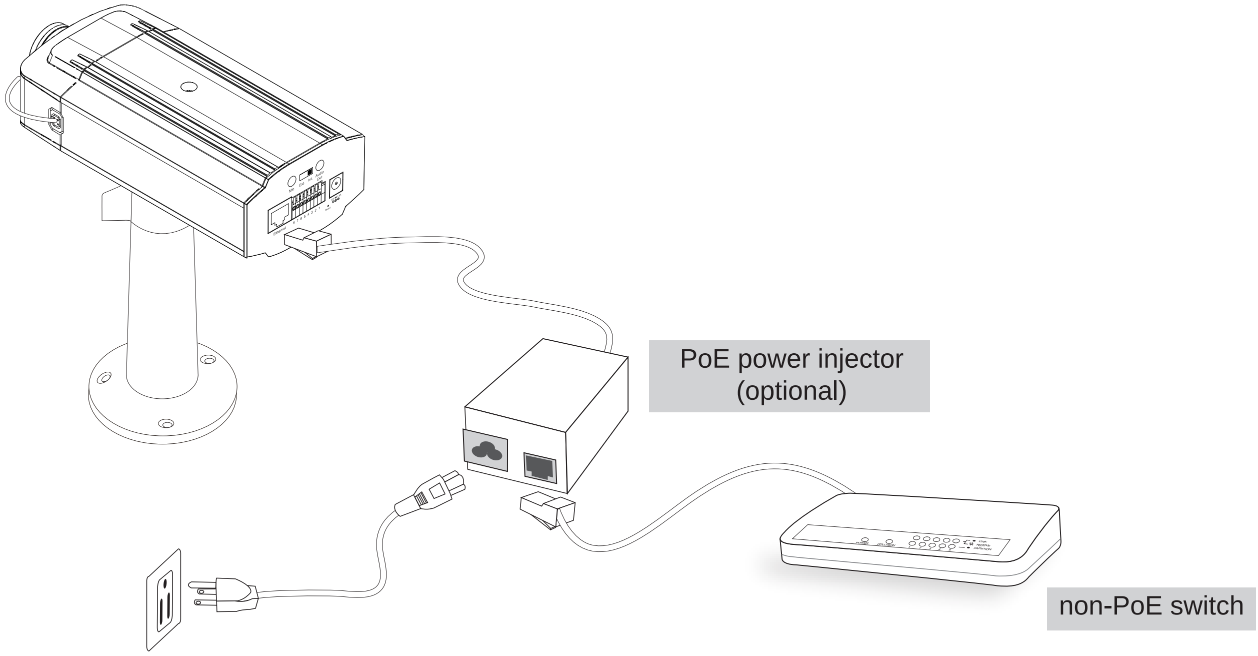
When using a PoE-enabled switch

The Network Camera is PoE-compliant, which allows it to be powered via a single Ethernet cable. If your switch/router supports PoE, refer to the following illustration to connect the Network Camera to a PoE-enabled switch/router via an Ethernet cable.



When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch/router.



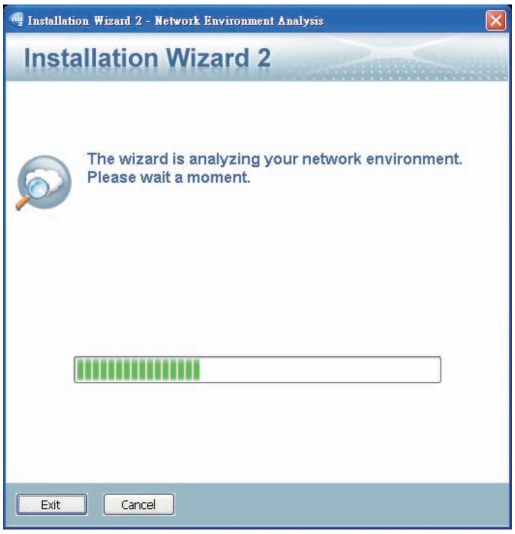
Software installation

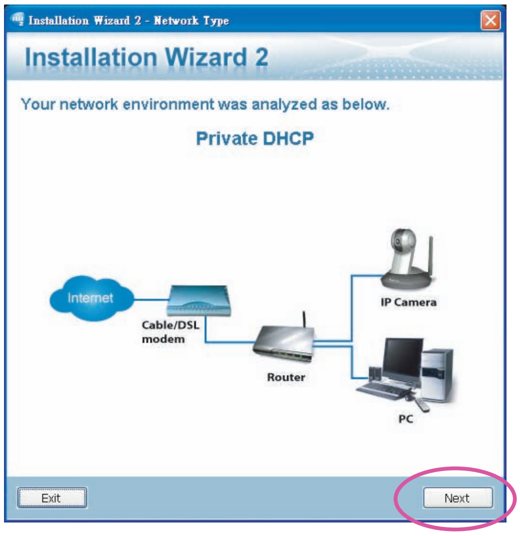
Installation Wizard 2 (IW2), free-bundled software packaged in the product CD, helps to set up your Network Camera in a LAN.

1. Install the IW2 under the Software Utility directory from the software CD.
   Double click the IW2 shortcut on your desktop to launch the program.



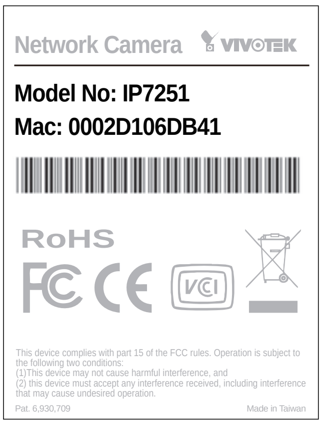
2. The program will conduct analyses on your network environment.
   After your network environment is analyzed, please click Next to continue the program.

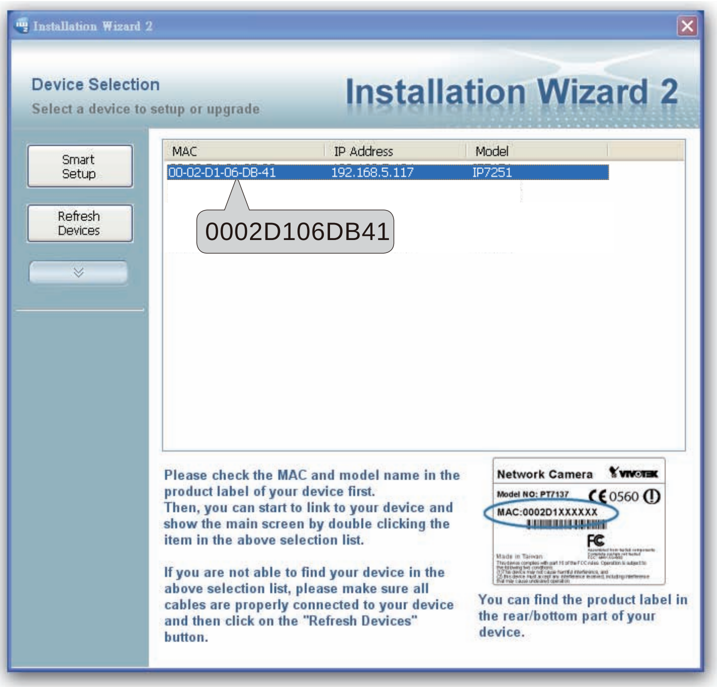




3. The program will search all VIVOTEK devices in the same LAN.

4. After searching, the main installer window will pop up. Click on the MAC and model name which match the product label on your device to connect to the Network Camera.



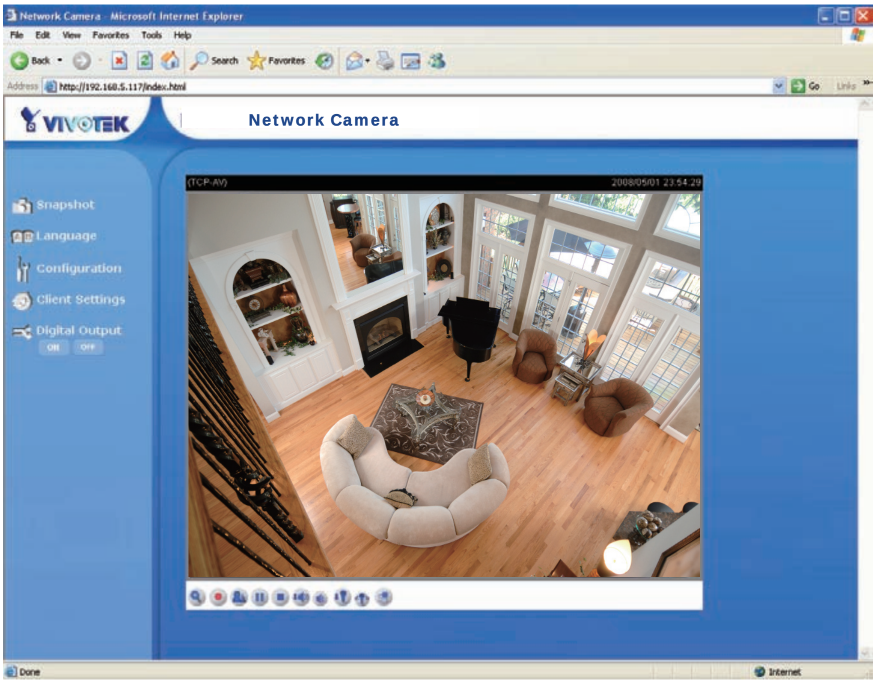


Accessing the Network Camera

This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

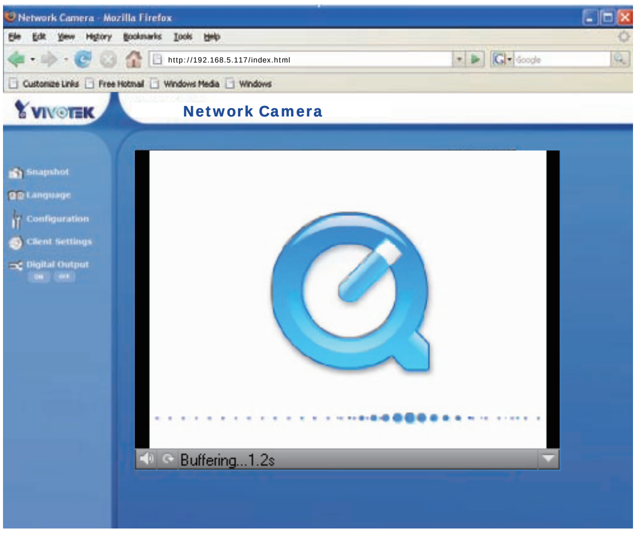
Using web browsers

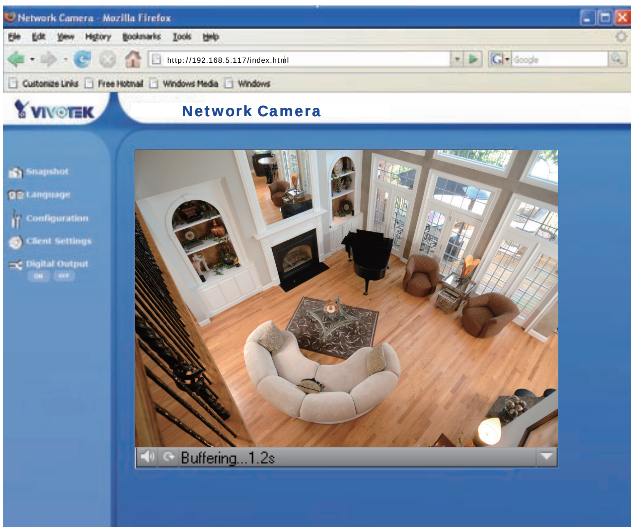
1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox or Netscape).
2. Enter the IP address of the Network Camera in the address field. Press Enter.
3. The live video will be displayed in your web browser.



NOTE

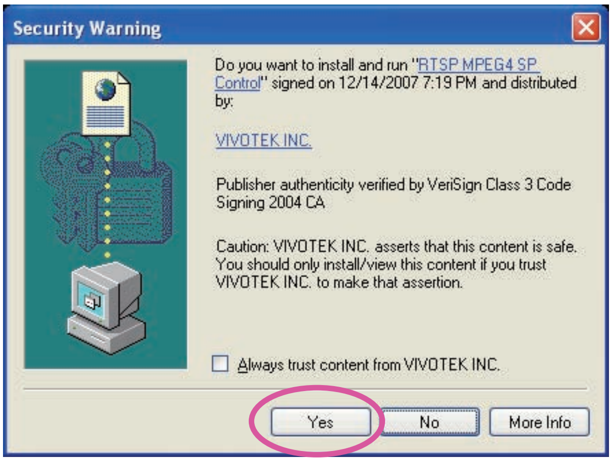
► *For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video.*





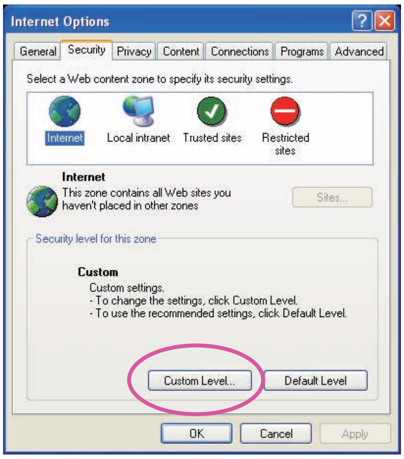
► *By default, the Network Camera is not password-protected. To prevent unauthorized accesses, it is highly recommended to set a password for the Network Camera.*
For more information about how to enable password protection, please refer to Security on page 23.

► *If you see a warning message at initial access, click Yes to install an ActiveX® control on your computer.*

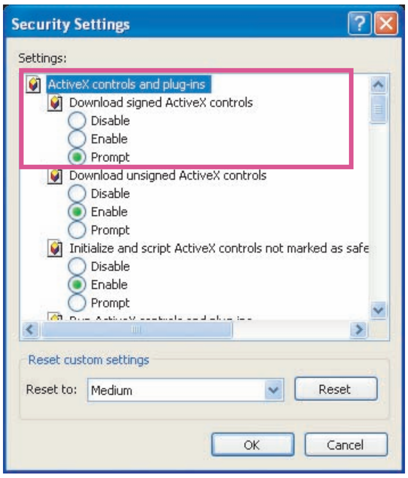


► *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable your ActiveX® Controls for your browser.*

1. Choose Tools > Internet Options > Security > Custom Level.



2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click OK.



Using RTSP players

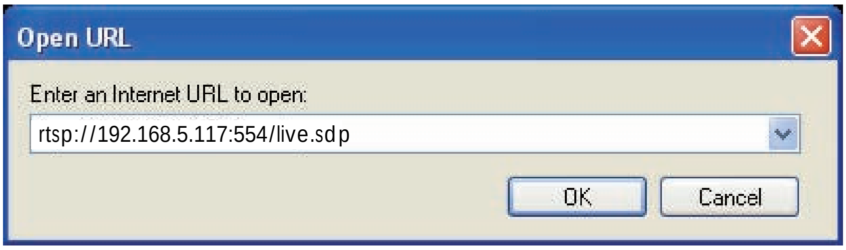
To view the MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

Quick Time Player

Real Player

1. Launch a RTSP player.
2. Choose File > Open URL. An URL dialog box will pop up.
3. Type the URL command in the text box.
   The format is rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>

   For example:



4. The live video will be displayed in your player.
   For more information on how to configure RTSP access name, please refer to RTSP Streaming on page 30 for details.



Using 3GPP-compatible mobile devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed from the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 7.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 30.

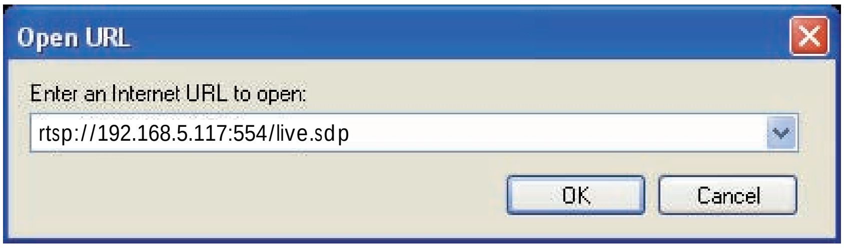
2. As the 3G network bandwidth is limited, you can't use large video size. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Audio and video on page 35.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (GSM-AMR)	12.2kbps

3. As most ISP and players only support port number 554 to allow RTSP streaming to go through, please set the RTSP port to 554.For more information, please refer to RTSP Streaming on page 30.

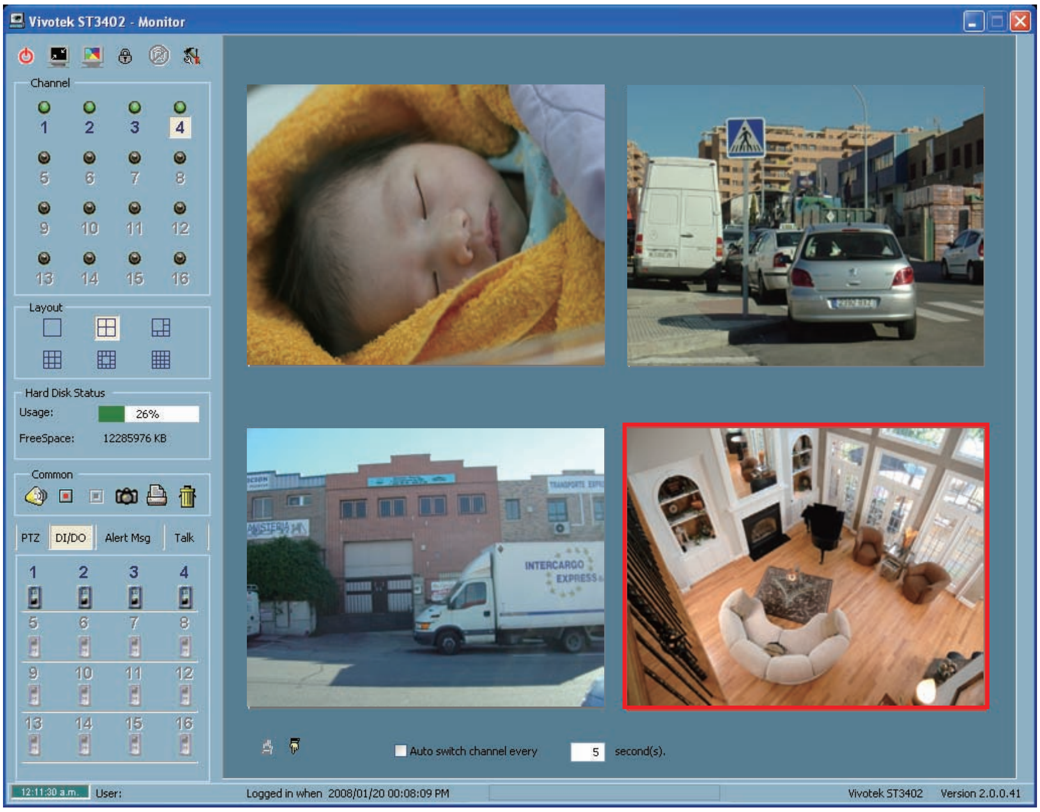
4. Launch the players on 3GPP-compatible mobile devices, (ex. Real Player).
   Type the URL commands in the player.
   The format is rtsp://<public ip address of your camera>:<rtsp port>/<access name for stream1 or stream2>.

   For example:



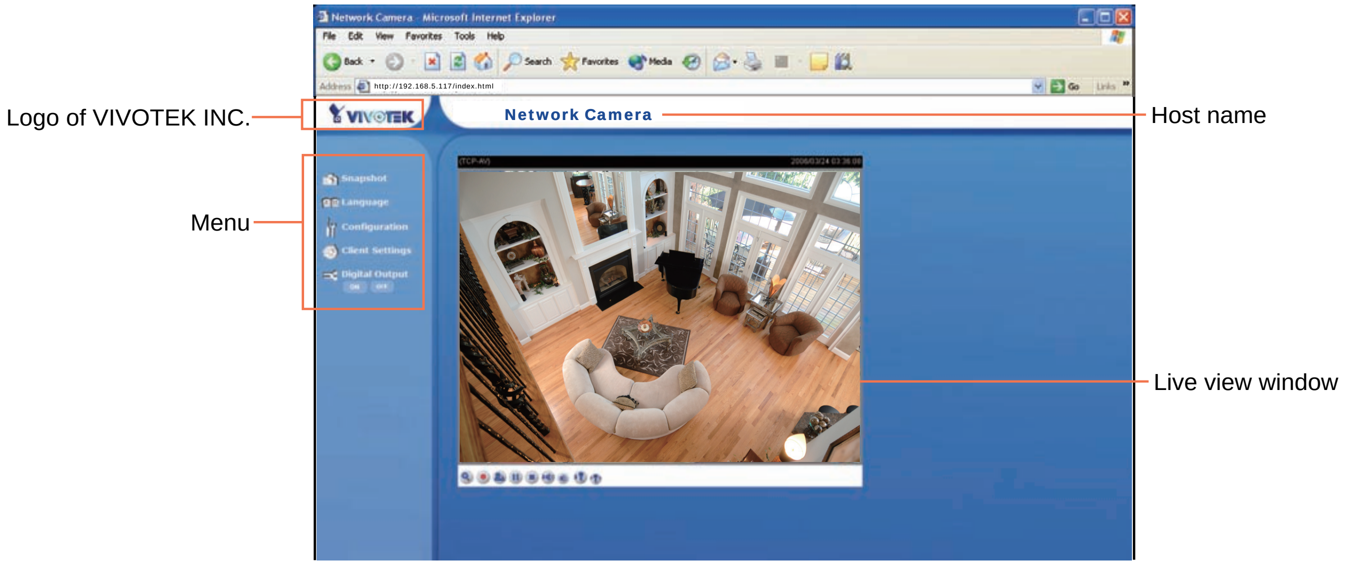
Using VIVOTEK recording software

The product software CD also contains recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software; then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download it at http://www.vivotek.com.



Main Page

This chapter explains the layout of the main page. It is composed of the following four sections: Logo of VIVOTEK INC., Menu, Host Name, and Live Video Window.



Logo of VIVOTEK INC.

Click this logo to visit VIVOTEK website.

Menu

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose Save Picture As to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Language: Click this button to choose a language for the displayed interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文 and 繁體中文.

Configuration: Click this button to access the configuration page of Network Camera. It is suggested that a password is applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 21.

Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 19.

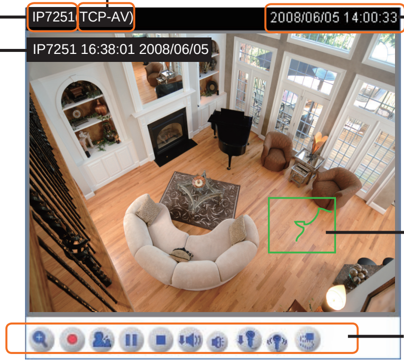
Digital Output: Click this button to turn on or off the digital output device.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 21.

Live Video Window

The following window is displayed when the video mode is set to MPEG-4:



Video title: The video title can be configured. For more information, please refer to Video settings on page 35.

Time: Display the current time. For more information, please refer to Video settings on page 35.

Title and time: Video title and time can be stamped on the streaming video. For more information, please refer to Video settings on page 35.

MPEG-4 protocol and media options: The transmission protocol and media options for MPEG-4 video streaming. For more information, please refer to Client Settings on page 19.

Video and audio control buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Digital zoom edit: Deselect Disable digital zoom to enable the zoom operation. The navigation screen indicates which part of the image is being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



Start MP4 recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 recording button to end recording. When you quit the web browser, video recording stops accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on page 20 for details.

Talk: Click this button to talk to people around the Network Camera. Audio will come out from the external speaker connected to the Network Camera.

Pause: Pause the transmission of streaming media. The button becomes Resume button after clicking the Pause button.

Resume: Resume the transmission of streaming media. The button becomes Pause button after clicking the Resume button.

Stop: Stop the transmission of streaming media. Click the Resume button to continue transmission.

Volume: When the mute function is not activated, move the slider bar to adjust the volume at local computer.

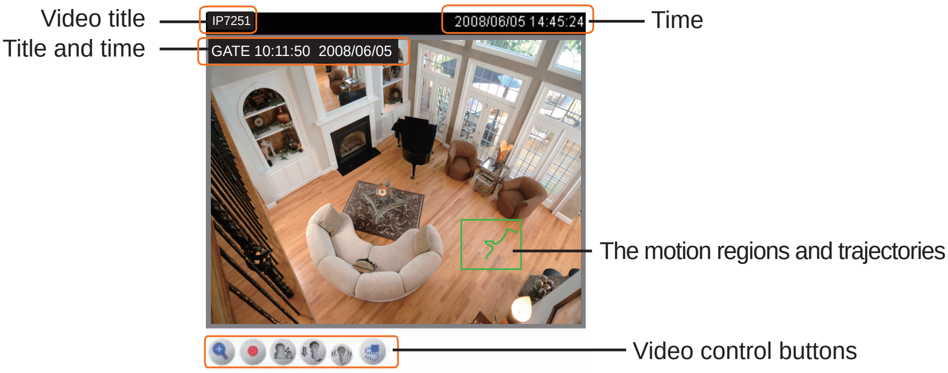
Mute: Turn off the volume at local computer.

Mic Volume: When the mute function is not activated, move the slider bar to adjust the microphone volume at local computer.

Mute: Turn off the microphone volume at local computer.

Show the motion regions and trajectories: Switch to the tracking mode. When a moving object is tracked, it will draw a curve of trajectory, which is the moving path of the tracked object. This button becomes Hide the motion regions and trajectories after clicking.

The following window is displayed when the video mode is set to MJPEG:



Video title: The video title can be configured. For more information, please refer to Video settings on page 35.

Time: Display the current time. For more information, please refer to Video settings on page 35.

Title and time: Video title and time can be stamped on the streaming video. For more information, please refer to Video settings on page 35.

Video and audio control buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Digital zoom edit: Deselect Disable digital zoom to enable the zoom operation. The navigation screen indicates which part of the image is being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



Start MP4 recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 recording button to end recording. When you quit the web browser, video recording stops accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on page 20 for details.

Talk: Click this button to talk to people around the Network Camera. Audio will come out from the external speaker connected to the Network Camera.

Mic Volume: When the mute function is not activated, move the slider bar to adjust the microphone volume at local computer.

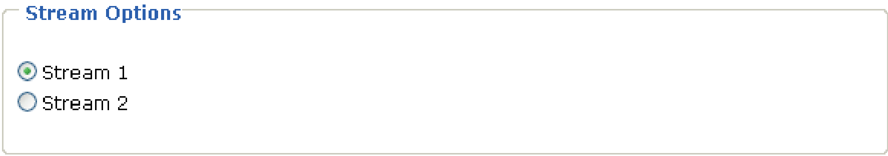
Mute: Turn off the microphone volume at local computer.

Show the motion regions and trajectories: Switch to the tracking mode. When a moving object is tracked, it will draw a curve of trajectory, which is the moving path of the tracked object. This button becomes Hide the motion regions and trajectories after clicking.

Client Settings

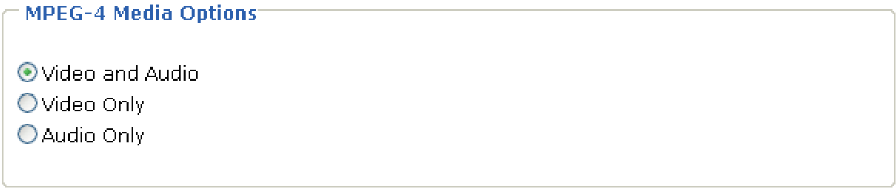
This chapter explains how to select the streaming source, transmission mode and saving options at local computer. It is composed of the following four sections: Stream Options, MPEG-4 Media Options, MPEG-4 Protocol Options and MP4 Saving Options. When completed with the settings on this page, click Save on the page bottom to take effect.

Stream Options



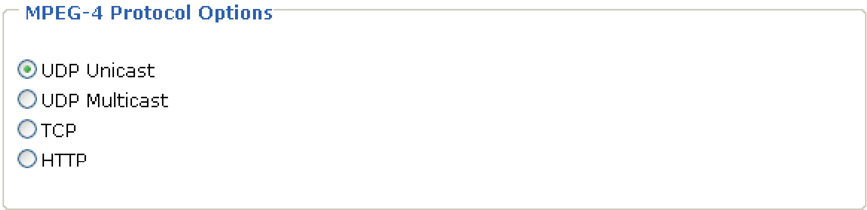
The Network Camera supports MPEG-4 and MJPEG dual streams. For more information, please refer to Video settings on page 35.

MPEG-4 Media Options



Select to stream video or audio data. This works only when the video mode is set to MPEG-4.

MPEG-4 Protocol Options



Depending on your network environment, there are four transmission modes of MPEG-4 streaming:

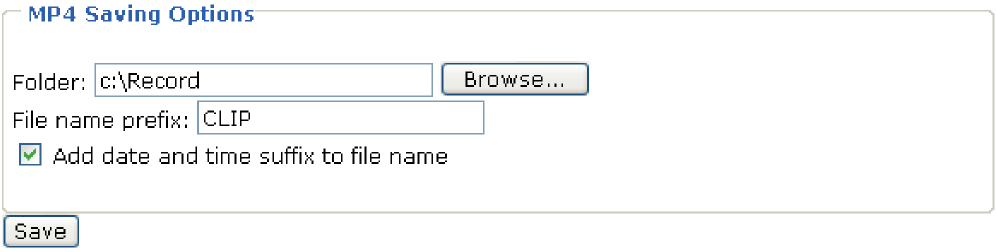
UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 30.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. Nevertheless, the downside with this protocol is that its real-time effect is not as good as that of the UDP protocol.

HTTP: This protocol allows the same quality as TCP protocol and you don't need to open specific port for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data to come through.

MP4 Saving Options

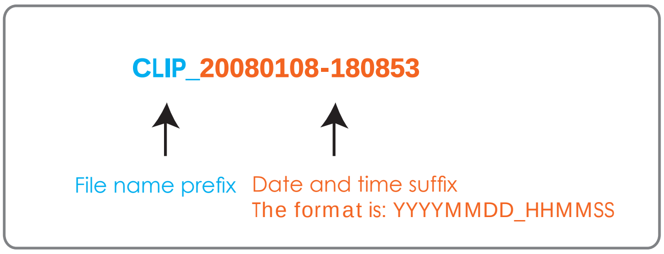


Users can record the live video as they are watching it by clicking Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

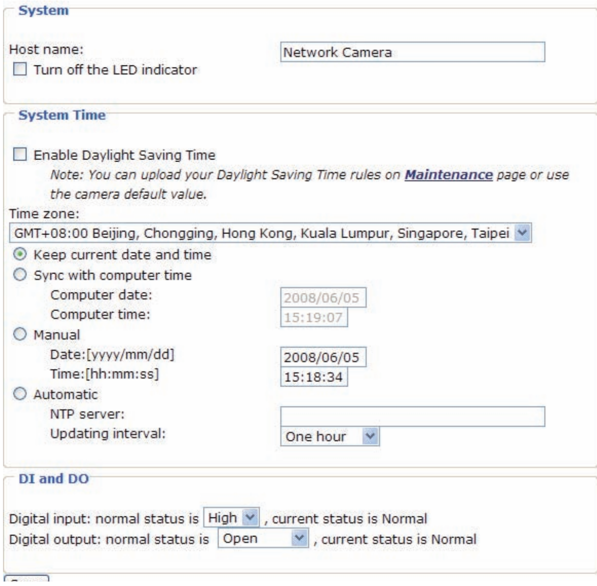
File Name Prefix: Enter the text that will be put in front of the video file name.

Add date and time suffix to the file name: Select this option to add date and time to the file name suffix.



Configuration

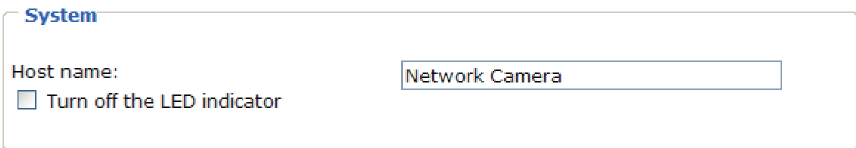
Only Administrators can access the system configuration page. Each category in the left menu will be explained in the following sections.



System

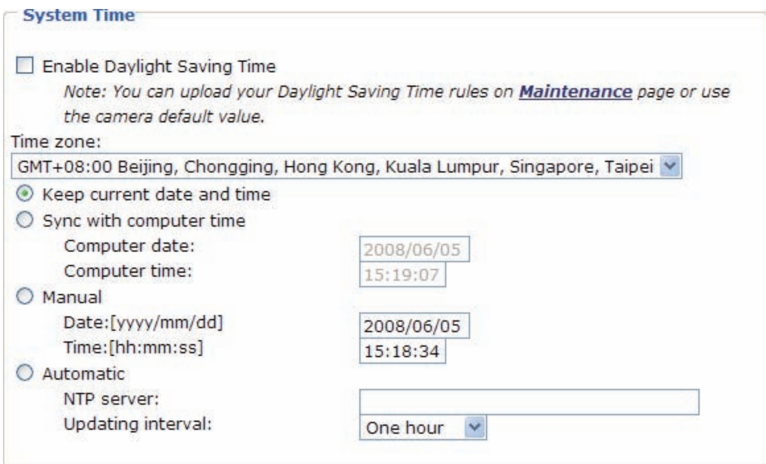
This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following three columns: System, System Time and DI and DO. When completed with the settings on this page, click Save on the page bottom to take effect.

System

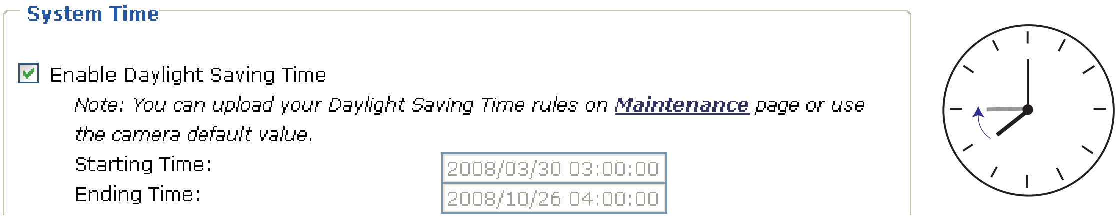


Host name: Set a desired name for the Network Camera. The text will be displayed at the top of the main page.

System Time



Enable Daylight Saving Time: Select this option to enable daylight saving time (DST). During DST, the system clock moves one hour ahead. Note that to utilize this feature, please set the time zone for your Network Camera first. Then, the starting time and ending time of the DST is displayed upon selecting this option. To manually configure the daylight saving time rules, please refer to Upload / Export Daylight Saving Time Configuration File on page 60 for details.



Time zone: According to your local time zone, select one from the drop-down list.

Keep current date and time: Select this option to reserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Sync with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

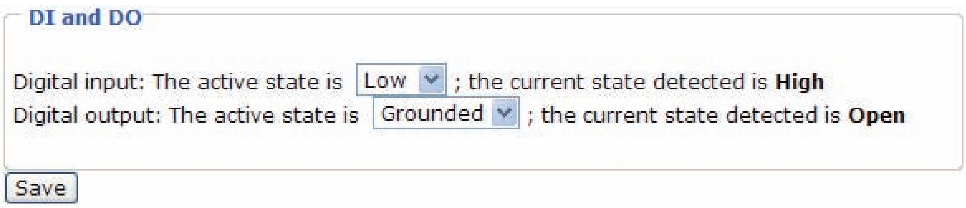
Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a protocol serves synchronize computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time-servers.

Update interval: Select to update the time with the NTP server on hourly, daily, weekly, or monthly basis.

DI and DO



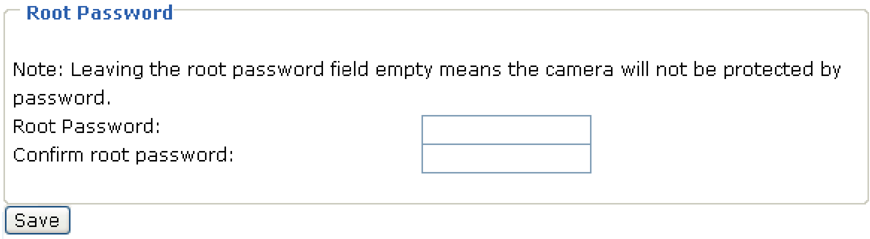
Digital input: Select High or Low to define normal status of the digital input. The Network Camera will report the current status.

Digital output: Select Grounded or Open to define normal status of the digital output. The Network Camera will show whether the trigger is activated or not.

Security

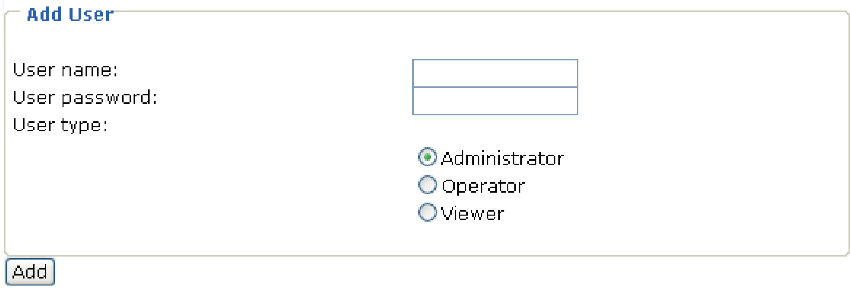
This section explains how to enable password protection and create multiple accounts. It is composed of the following three columns: Root Password, Add User and Manage User.

Root Password



The administrator account “root” is permanent and can not be deleted. Please note that if you want to add more accounts, you must apply a password for the “root” account first.
1. Type the password identically in both text boxes.
2. Click Save to enable password protection.
3. A window will be prompted for authentication; type the correct user’s name and password in related fields to access the Network Camera.

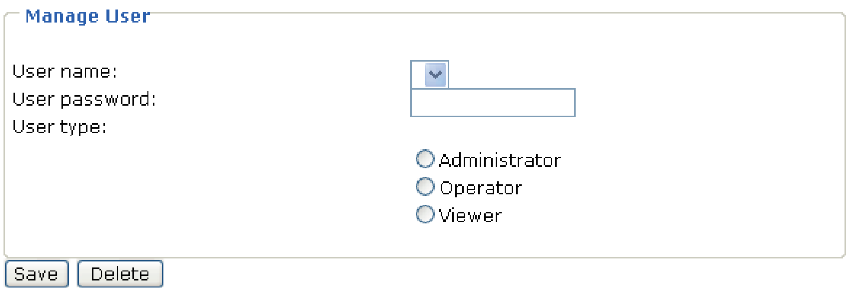
Add User



Administrators can add up to twenty user accounts.
1. Input the new user’s name and password.
2. Select the desired security level. Click Add to take effect.

Access rights are sorted by user types. There are three kinds of user types. Only administrators can access the Configuration page. Operators and viewers can not access the configuration page. Though operators can not access the page, they are capable of using the url commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 63. Viewers can only access the main page.

Manage User

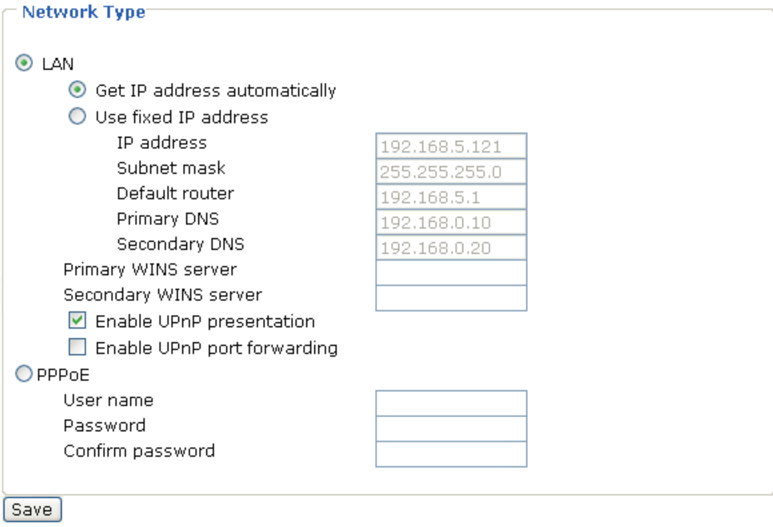


Here you can change user’s access rights or delete user accounts.
1. Pull down the user list to find an account.
2. Make necessary changes and then click Save or Delete to take effect.

Network

This section explains how to configure wired network connection for the Network Camera. It is composed of the following five columns: Network Type, HTTP, Two way audio, FTP and RTSP Streaming. When completed with the settings on this page, click Save to take effect.

Network Type



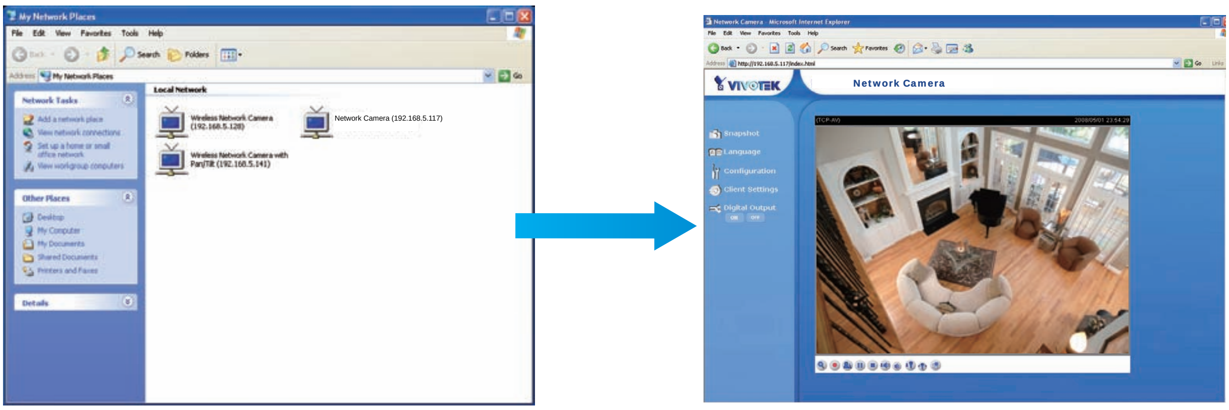
LAN

Select this option when the Network Camera is deployed in a local area network (LAN) and is intended to be accessed by local computers.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by a DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera. Please refer to Internet connection with static IP on page 8 for details.

Enable UPnP presentation: Select this option to enable UPnP™ presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras will be listed in My Network Places. Currently, UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP™ component is installed on your computer.



Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnPTM and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

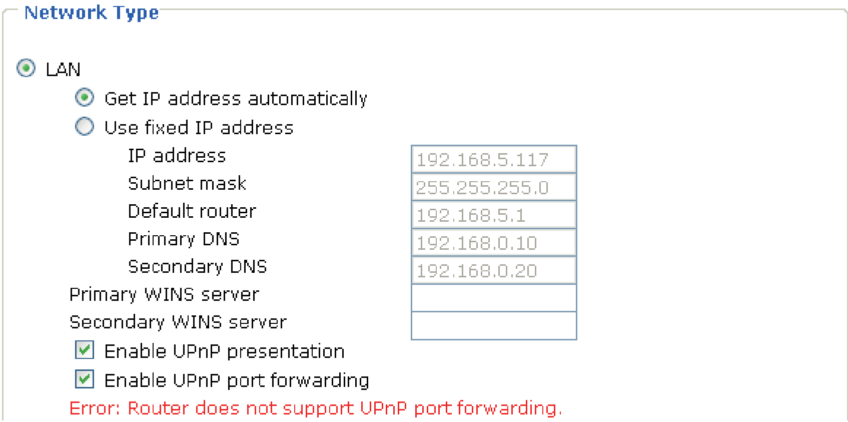
Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera in a LAN.
2. Go to Configuration > Application > Server Settings (please refer to Server Settings on page 48) to add a new server -- email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 46). Select System log so that you will receive a list of system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password provided by your ISP. Click Save to take effect.
5. The Network Camera starts to reboot.
6. Disconnect the power source of the Network Camera; remove it from the LAN environment to the Internet.

NOTE

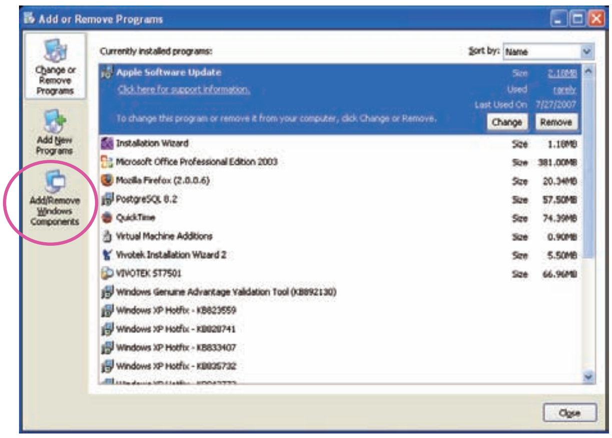
► *If the default ports are already used by other device connecting to the same router, the Network Camera will select other ports for the Network Camera.*

► *If UPnP™ is not supported by your router, you will see the following message.*

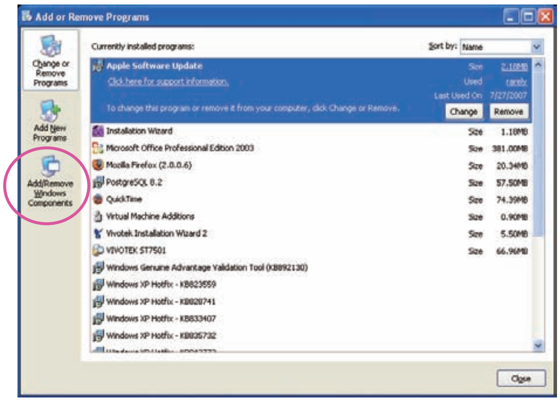


► *Steps to enable UPnP™ user interface on your computer:*
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

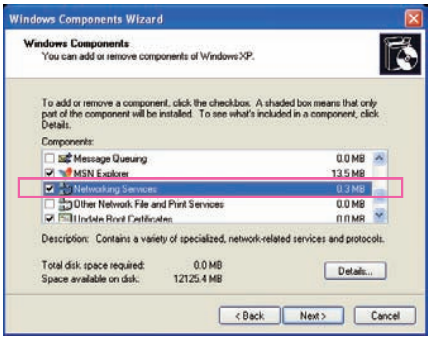
1. Go to Start, click Control Panel, and then click Add or Remove Programs.



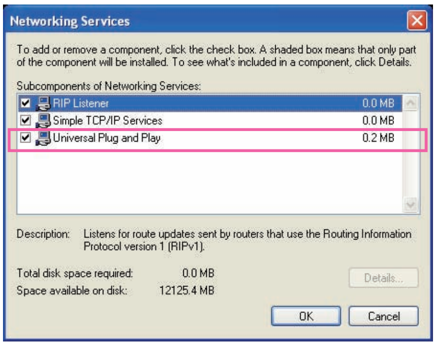
2. In the Add or Remove Programs dialog box, click Add/Remove Windows Components.



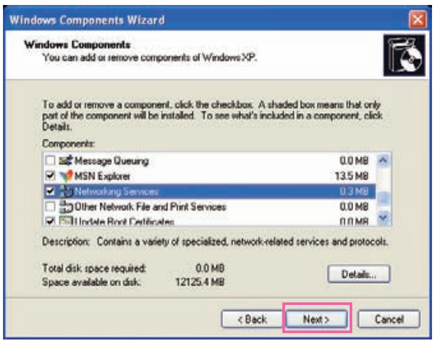
3. In the Windows Components Wizard dialog box, select Networking Services and then click Details.



4. In the Networking Services dialog box, select Universal Plug and Play and then click OK.



5. Click Next in the following window.



6. Click Finish. UPnP™ is enabled.

► How does UPnP™ work?

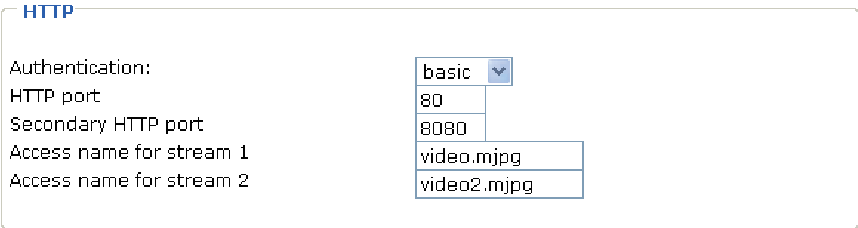
UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without bothersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts at My Network Places.

► *Enabling UPnP port forwarding allows the Network Camera to open secondary HTTP port on the router, not HTTP port, meaning that you have to add the secondary HTTP port number behind the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.*

From the Internet	In a LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 59 for details. After the Network Camera is reset to factory default, it is accessible in a LAN.*

HTTP



Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for a HTTP transaction: basic and digest. If basic authentication is selected, the password is sent in plain text format; there can be potential risks of being intercepted. If digest authentication is selected, user credentials are encrypted in MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. Also, they can be assigned with another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages are displayed:



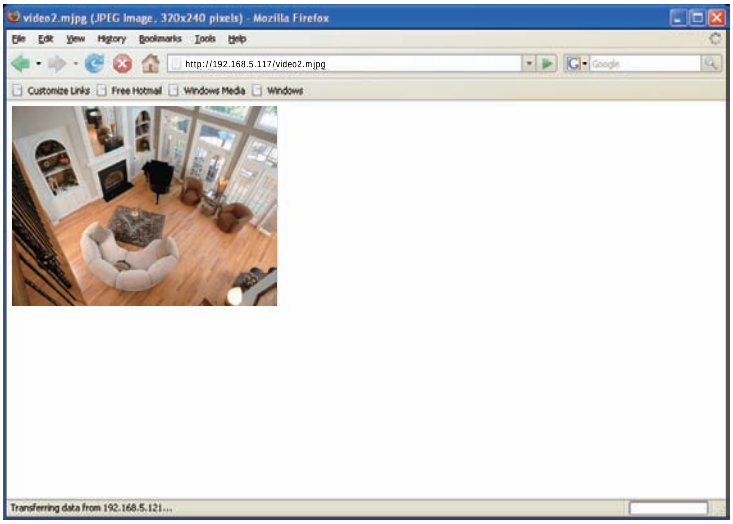


To access the Network Camera within a LAN, both HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

In a LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for stream 1 / Access name for stream 2: The access name is used to differentiate the streaming source. When using Mozilla Firefox or Netscape to access the Network Camera, and the video mode is set to JPEG, users will receive continuous JPEG pictures. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.
Use http://<ip address>:<http port>/<access name for stream1 or stream2> to make connection.

For example, when the access name for stream 1 is set to video.mjpg:
1. Launch Mozilla Firefox or Netscape.
2. Type the URL command in the address field. Press Enter.
3. The JPEG images will be displayed in your web browser.



NOTE

► *To utilize the HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security on page 23 for details.*

► *Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream1 or stream2> will fail to access the Network Camera.*

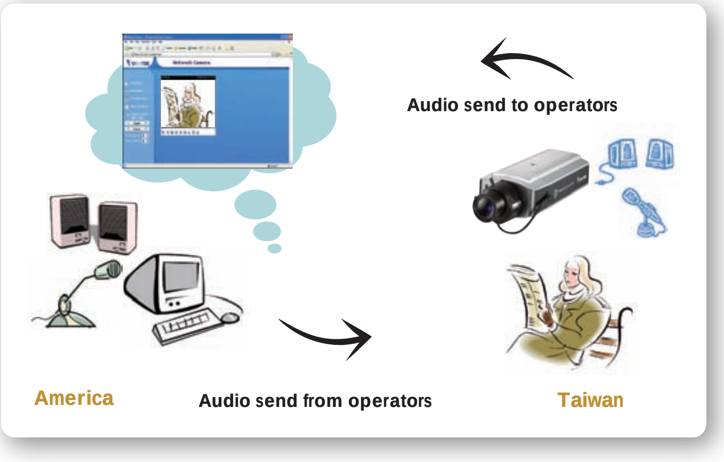
Two way audio

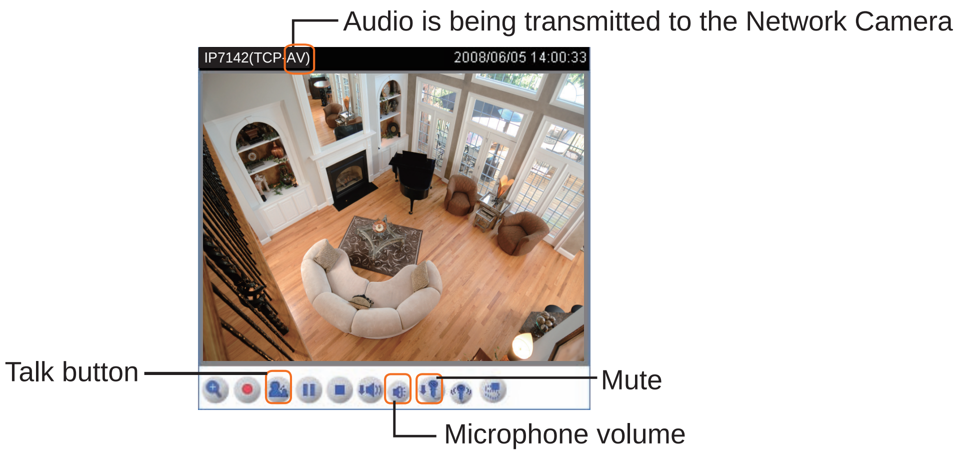


By default, the two way audio port is set to 5060. Also, it can be assigned with another port number between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in microphone and an external speaker, you can communicate with people around the Network Camera.

Note that as JPEG only transmits a series of JPEG images to the client, to utilize this feature, make sure the video mode is set to "MPEG-4" and the media option is set to "Video and Audio".





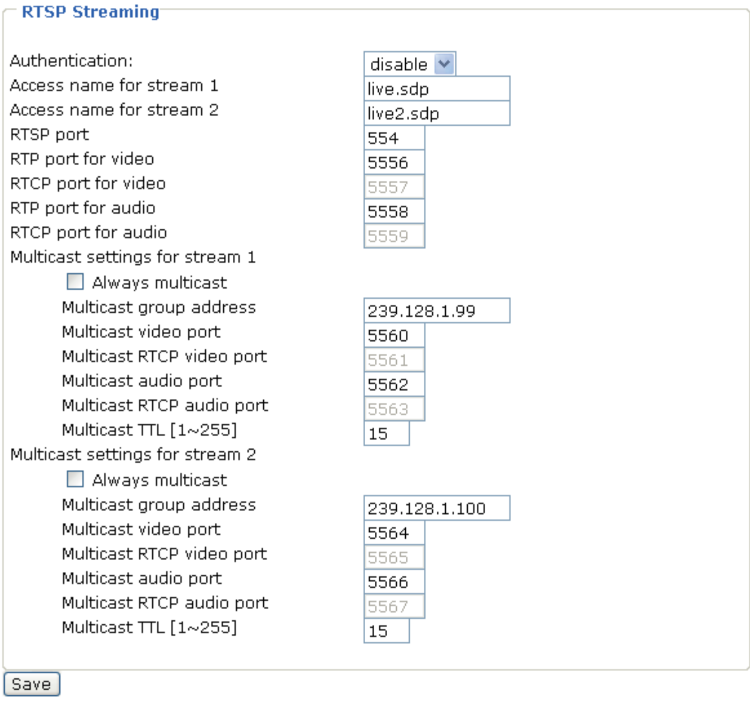
Click to enable audio transmission to the Network Camera; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

FTP



The FTP server allows the Network Camera to utilize VIVOTEK Installation Wizard 2 to upgrade firmware. By default, the FTP port is set to 21. Also, it can be assigned with another port number between 1025 and 65535.

RTSP Streaming



Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic and digest. If basic authentication is selected, the password is sent in plain text format; there can be potential risks of being intercepted. If digest authentication is selected, user credentials are encrypted in MD5 algorithm and thus provide better protection against unauthorized accesses.

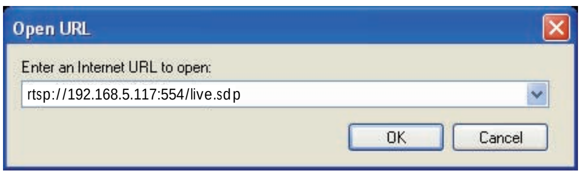
The accessibility of the RTSP streaming for the three authentication modes are listed in the following table:

	Quick Time player	Real Player
Disable	O	O
Basic	O	O
Digest	O	X

O indicates that the authentication mode is supported by the RTSP player.
X indicates that the authentication mode is NOT supported by the RTSP player.

Access name for stream 1 / Access name for stream 2: The access name is used to differentiate the streaming source. When using a RTSP player to access the Network Camera, and the video mode is set to MPEG-4, use the following RTSP URL command to request a transmission of streaming data.

rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>
For example, when the access name for stream 1 is set to live.sdp:
1. Launch a RTSP player.
2. Choose File > Open URL. An URL dialog box will pop up.
3. Type the URL command in the text box.
   For example:



4. The live video will be displayed in your player.



RTSP port /RTP port for video, audio/ RTCP port for video, audio

The RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The five ports can be changed between 1025 and 65535. The RTP port must be an even number and the RTCP port is RTP port number plus one, and thus always be odd. When the RTP port changes, the RTCP port will change accordingly.

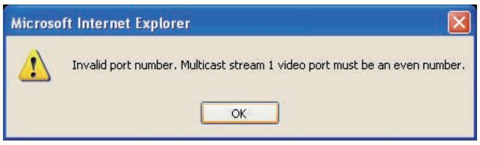
If the RTP ports are incorrectly assigned, the following warning message is displayed:



Multicast settings for stream 1 / Multicast settings for stream 2: Select the Always multicast to enable multicast for stream 1 or stream 2. Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream by requesting a copy from the Multicast group address.

The five ports can be changed between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus it is always be odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message is displayed:



Multicast TTL [1~255]:The multicast TTL (Time to live) is the value that tells the router the range a packet can be forwarded.

NOTE

► *To utilize the RTSP streaming authentication, make sure that your have set a password for the Network Camera first; please refer to Security on page 23 for details.*

DDNS

This section explains how to configure dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

DDNS: Dynamic domain name service

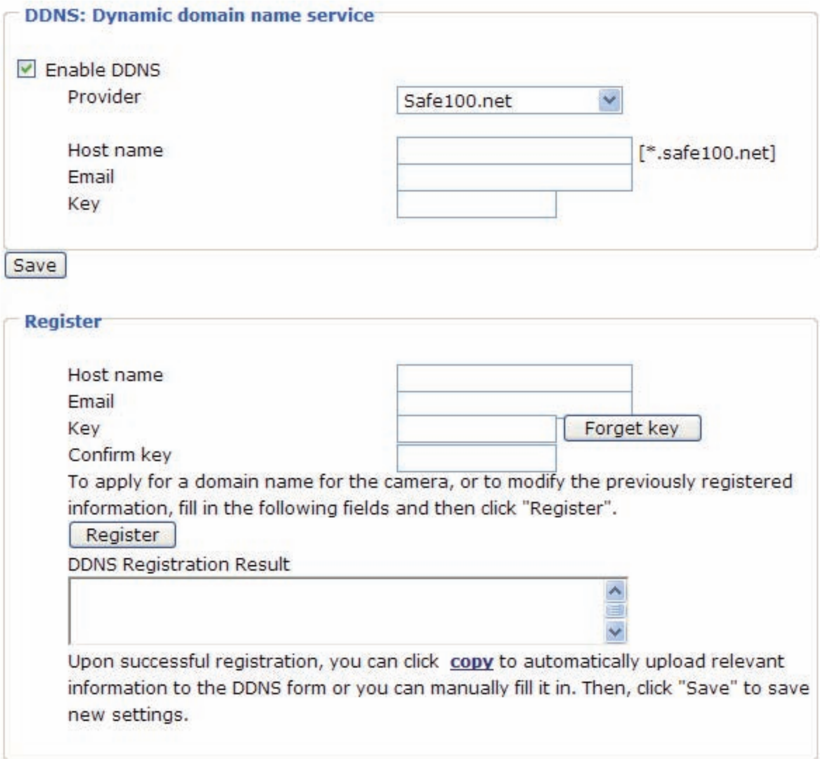


Enable DDNS: Select this option to enable the DDNS setting.

Provider: Select a DDNS provider of your choice from the Provider drop-down list.
VIVOTEK offers safe100, a free dynamic domain name service to VIVOTEK customers. It is recommended that you register with the safe100 to access the Network Camera from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it. Note that to utilize this feature, please apply a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select Safe100 from the Provider drop-down list. Click Agree when you agree with the terms of the Service Agreement.
2. In the Register column, fill in the Host name, Email, Key and Confirm Key and then click Register. After a host name has been successfully created, you will see a successful message in the DDNS Registration Result column, indicating that you have successfully applied a domain name on Safe100.net.



3. Click Copy and all the registered information will be uploaded to the corresponding fields in the DDNS column.



4. Select Enable DDNS and then click Save to take effect.

■ CustomSafe100

VIVOTEK offers documents to establish CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the Provider drop-down list.
2. In the Register column, fill in the Host name, Email, Key and Confirm Key; then click Register. After a host name has been successfully created, you will see a successful message in the DDNS Registration Result column, indicating that you have successfully registered a domain name on CustomSafe100.
3. Click Copy and all the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and then click Save to take effect.

Forget key: Click this button if you forget the key of Safe100 or CustomSafe100. Your account information will be sent to your email address.

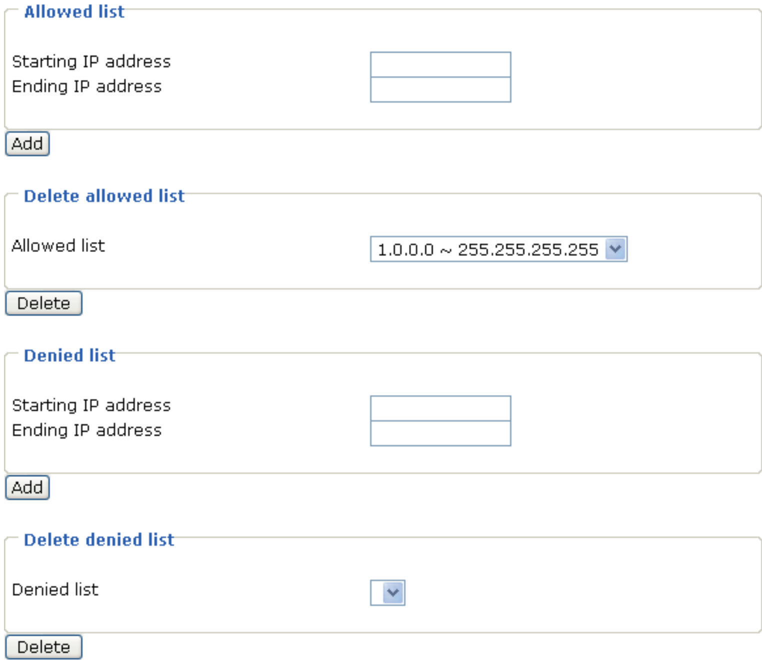
Refer to the following links to apply a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/
■ TZO.com: visit http://www.tzo.com/
■ DHS.org: visit http://www.dhs.org/
■ dyn-interfree.it: visit http://dyn-interfree.it/

Access list

This section explains how to control the access permission by checking the client PC's IP addresses. It is composed of the following four columns: Allowed list, Denied list, Delete allowed list, and Delete denied list.

Allowed list / Denied list

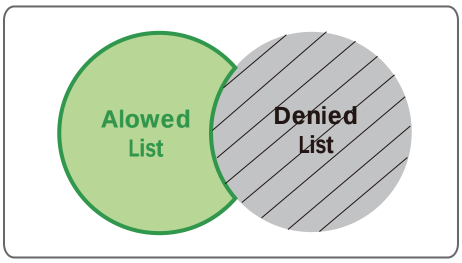


There are two lists for permission control: Allowed list and Denied list. Only those clients whose IP addresses are in the Allowed list and not in the Denied list can access the Network Camera.

1. In the Allowed list or Denied list column, type the starting IP address and ending IP address in the text boxes. A total of ten lists can be configured for both columns.
2. Click Add to take effect.

NOTE

► *For example, when the range of allowed list is set from 1.1.1.0 to 192.255.255.255 and the range of denied list is set from 1.1.1.0 to 170.255.255.255, Only users' IP located between 171.0.0.0 and 192.255.255.255 can access the Network Camera.*



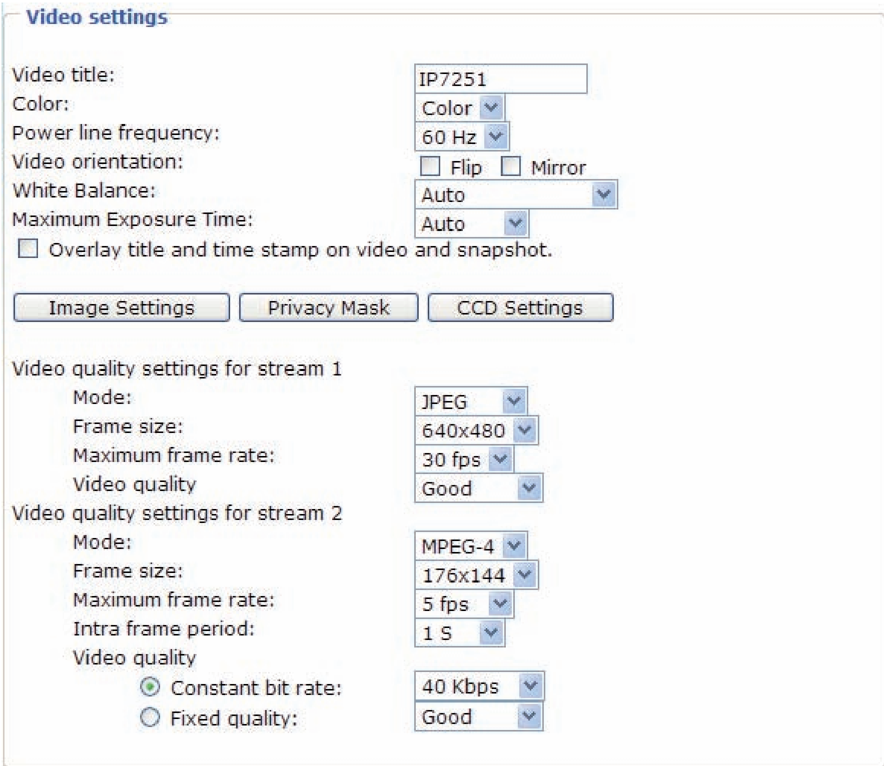
Delete allowed list / Delete denied list

1. In the Delete allowed list or Delete denied list, select a list from the drop-down list.
2. Click Delete to take effect.

Audio and video

This section explains how to cofigure audio and video performances of the Network Camera. It is composed of the following two columns: Video settings and Audio settings.

Video settings



Video title: Enter a name that will be displayed on the title bar of the live video.



Color: Select to display colorful or black/white video streams.

Power line frequency: Set the power line frequency in consistent with local utility settings to eliminate uncomfortable image flickering associated with fluorescent lights. Note that after the power line frequency is changed, it is required to disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling) to correct the image orientation.

White balance: Adjust the value for best color temperature.

■ Auto
The Network Camera automatically adjusts the color temperature of light in response to different light sources. The white balance setting defaults to Auto and works well in most situations.

■ Fixed indoor: about 2800K

■ Fixed fluorescent: about 4000K

■ Fixed outdoor: about 6500K

Maximum Exposure Time: 1/120 S, 1/60 S, 1/30 S, 1/15 S, and Auto.

Overlay title and time stamp on video: Select this option to place the video title and time on video streams.
Note that when the frame size is set to 176 x 144 as the right picture below, only time will be stamped on video streams.



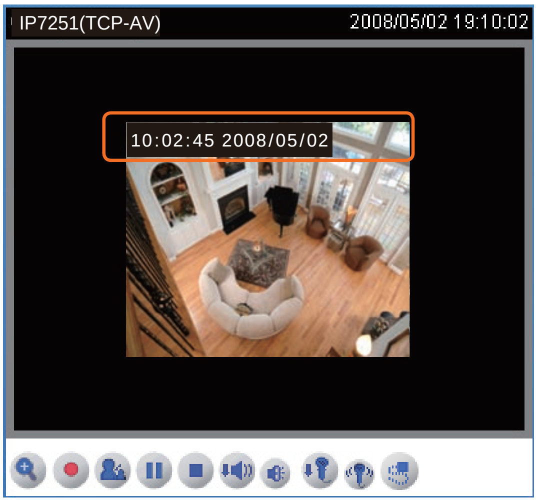
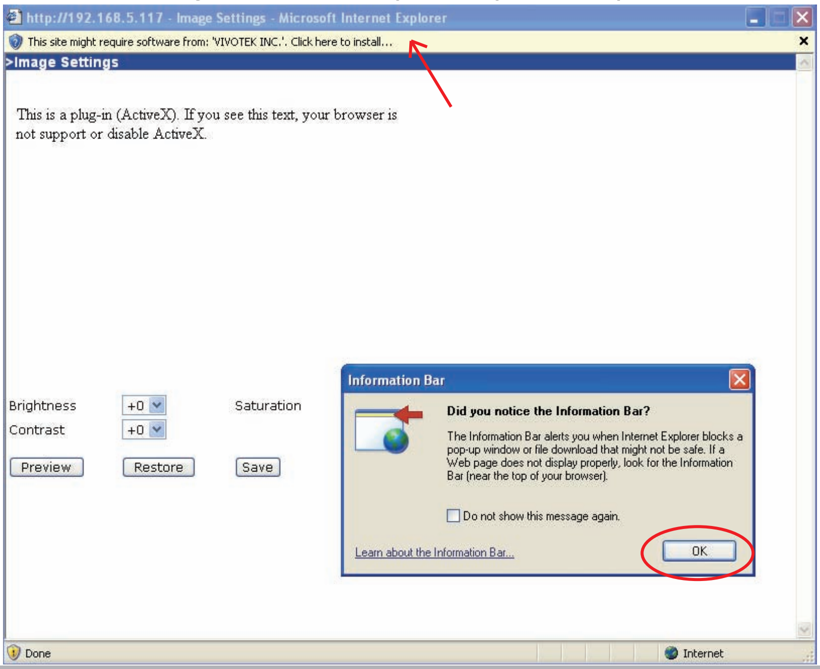
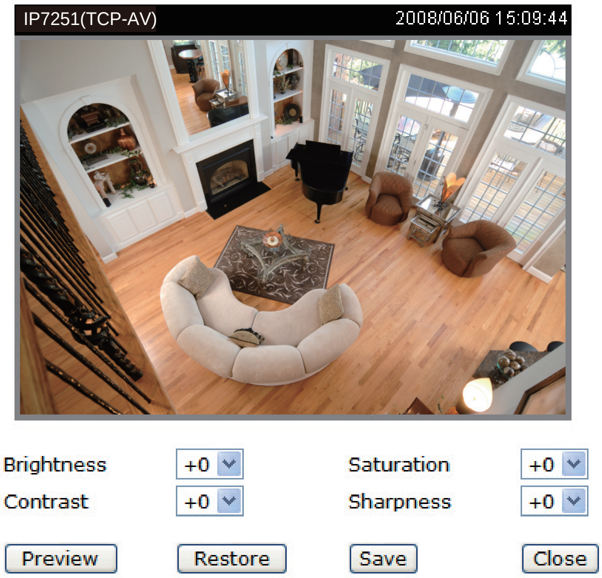


Image Settings
Click Image settings to open the Image Settings page.
If you see a warning message as below, click Yes and then the information bar on the top of the page to install an ActiveX® control for Intelligent Video Analysis on your computer.

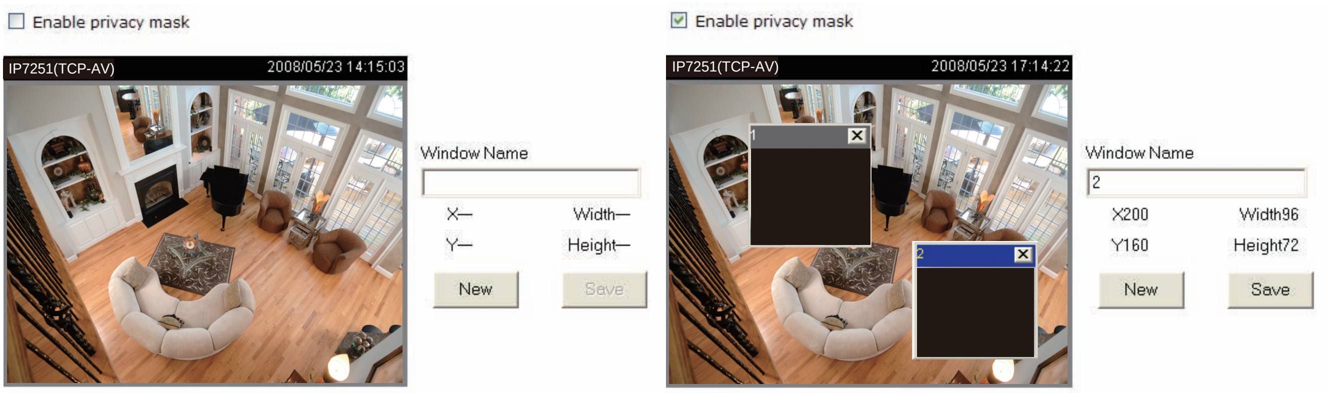


In this page, you can tune Brightness, Saturation, Contrast for video compensation. In this page, you can tune brighness, contrast, saturation, and sharpness for video compensation. Each field of brightness, contrast and saturation has eleven levels ranged from -5 to +5, and has seven levels ranged from -3 to +3 for sharpness.
You can click Preview to fine-tune the image, or click Restore to recall the original settings without incorporating the changes. When completed with the settings on this page, click Save to take effect and click Close to quit the page.



Privacy mask

Click Privacy Mask to open the Privacy Mask page. In this page, you can block out some sensitive zones for privacy concerns.



■ To set the privacy mask windows, follow the steps below:
1. Click New to add a new window.
2. To resize and drag-drop the window, which is recommended to be at least twice the size of the object (height and width) you want to cover.
3. Enter a descriptive Window Name and click Save to take effect.
4. Select Enable privacy mask to enable this function.

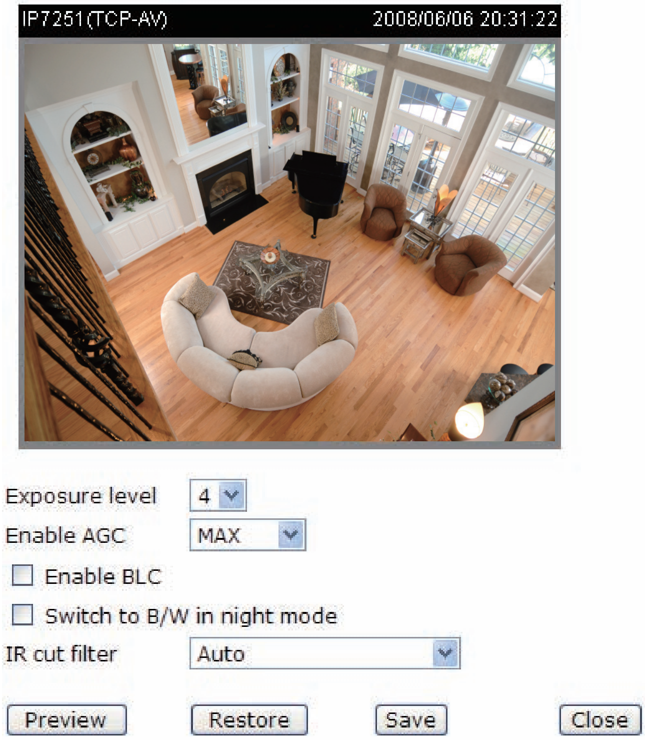
NOTE

► *Up to 5 privacy mask windows can be set in the same screen.*

► *If you want to delete the window, please click on the 'x' at the upper right-hand corner of the window to close the window.*

CCD Settings

Click CCD settings to open the CCD Settings page. In this page, you can set the exposure level, enable AGC, enable BLC functions. night mode, and IR cut filter.



Exposure level:
You can manually set up the Exposure level, which ranges from 1 to 8. The default value is 4.

Enable AGC (Auto Gain Control):
You can manually set up the AGC level (MAX or Normal).

Enable BLC (Back Light Compensation)
Enable it when the object is too dark or too bright to recognize. It allows the camera to adjust to the best light conditions in any environment and automatically give the necessary light compensation.

Switch to B/W in night mode:
Select it to enable the Network Camera to automatically switch to B/W in night mode.

IR cut filter:
With a removable IR-cut filter and built-in IR illuminators, up to 15m, this Network Camera can automatically remove the filter and turn on the IR illuminators during the nighttime to accept IR illumination for low light sensitivity.

■ Auto
The Network Camera automatically removes the filter by judging the level of ambient light.

■ Schedule mode
The Network Camera switches between day mode and night mode based on specified schedule. Enter the starting time and ending time for the day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the starting time and ending time of day mode are set to 07:00 and 18:00.

■ Day mode
In day mode, the Network Camera switches on the IR cut filter at all times to block the infrared light from reaching the sensor so that the colors will not be distorted.

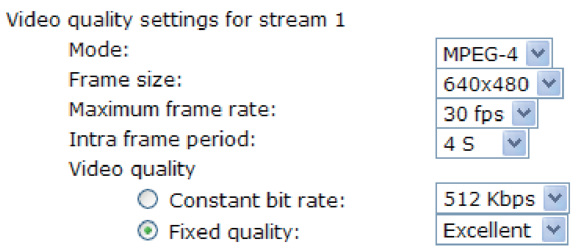
■ Night mode
In night mode, the Network Camera switches off (remove) the IR cut filter to allow the infrared light to pass through. This improves the sensitivity of the Network Camera in low-light conditions.

You can click Preview to fine-tune the image, or click Restore to recall the original settings without incorporating the changes. When completed with the settings on this page, click Save to take effect and click Close to quit the page.

Video quality settings for stream 1 / stream 2: You can set up two seperate streams for the Network Camera for different viewing devices. For example, set the Network Camera to a smaller frame size and a lower bit rate for remote viewing on mobile phones. Or, set the Network Camera to a larger video size and a higher bit rate for live viewing on web browsers.

■ Mode
The Network Camera offers two choices of video compression standards for real-time viewing: MPEG-4 and MJPEG.

If MPEG-4 is selected, it is streamed in RTSP protocol. There are four dependent parameters provided in MPEG-4 mode for video performance adjustment.



■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: 176 x 144, 320 x 240 and 640 x 480.

■ Maximum frame rate
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video quality.

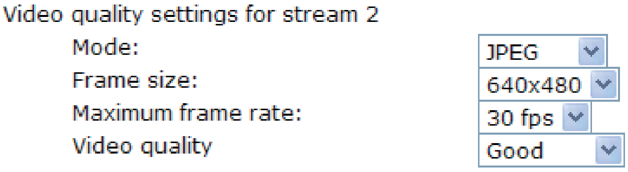
If the power line frequency is set to 50Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps and 30fps.

■ Intra frame period
Determine how often to plant an I frame. The shorter the duration, the more likely you will get a better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following duration: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds and 4 seconds.

■ Video quality
A complex scene generally produces larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if Constant bit rate is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performances. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps and 4Mbps.

On the other hand, if Fixed quality is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video qualities are selectable at the following settings: Medium, Standard, Good, Detailed and Excellent.

If JPEG mode is selected, the Network Camera continuously sends JPEG images to the clients, producing dynamic effects similar to movies. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. And because the media contents are a combination of JPEG images, no audio data is transmitted to the clients.



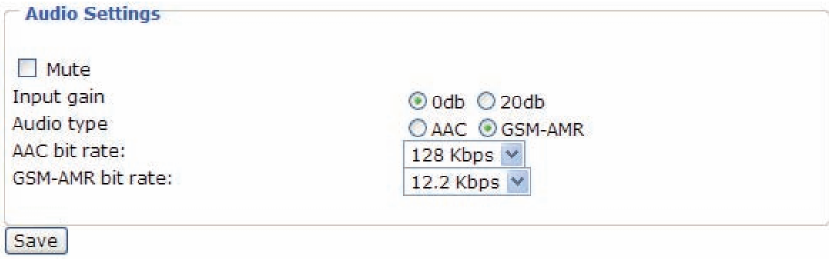
■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: 176 x 144, 320 x 240 and 640 x 480.

■ Maximum frame rate
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video quality.

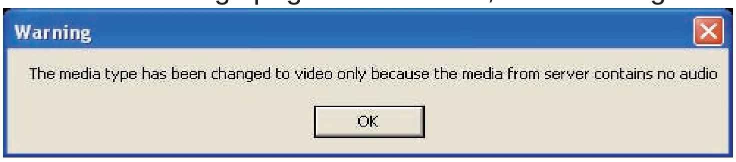
If the power line frequency is set to 50Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps and 30fps.

■ Video quality
The video qualities are selectable at the following settings: Medium, Standard, Good, Detailed and Excellent.

Audio settings



Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if mute mode is turned on, no audio data will be transmitted to all clients even though the audio transmission is enabled in the Client Settings page. In that case, the following message is displayed.



Input gain: There are two options for external microphone input gain, 0db and 20db.

Audio type: Select audio codec AAC or GSM-AMR and the bit rate.
■ AAC targets at performing good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable at the following rates: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps and128Kbps.

■ GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable at the following rates: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps and 12.2Kbps.

When completed with the settings on this page, click Save to take effect.

Motion detection

This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.



To enable motion detection, follow the steps below:

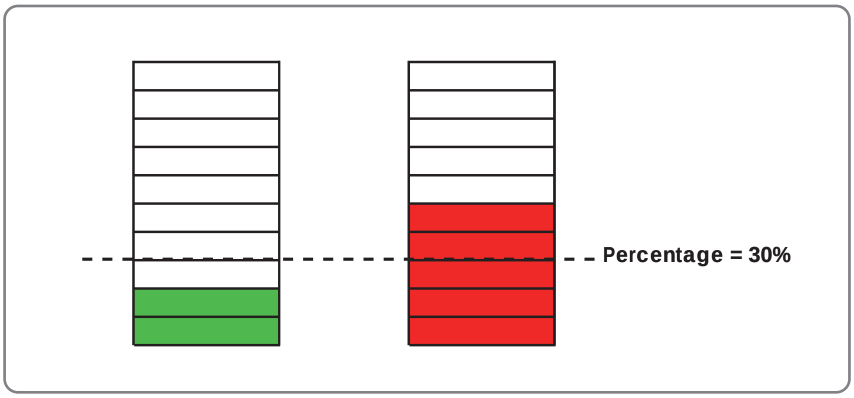
1. Click New to add a new motion detection window.
2. In the Window Name text box, enter a descriptive name for the motion detection window.
   ■ To move and resize the window, drag-drop the window.
   ■ To delete window, click X at top right of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slider bar.
4. Click Save to take effect.
5. Select Enable motion detection to enable this function.

For example:



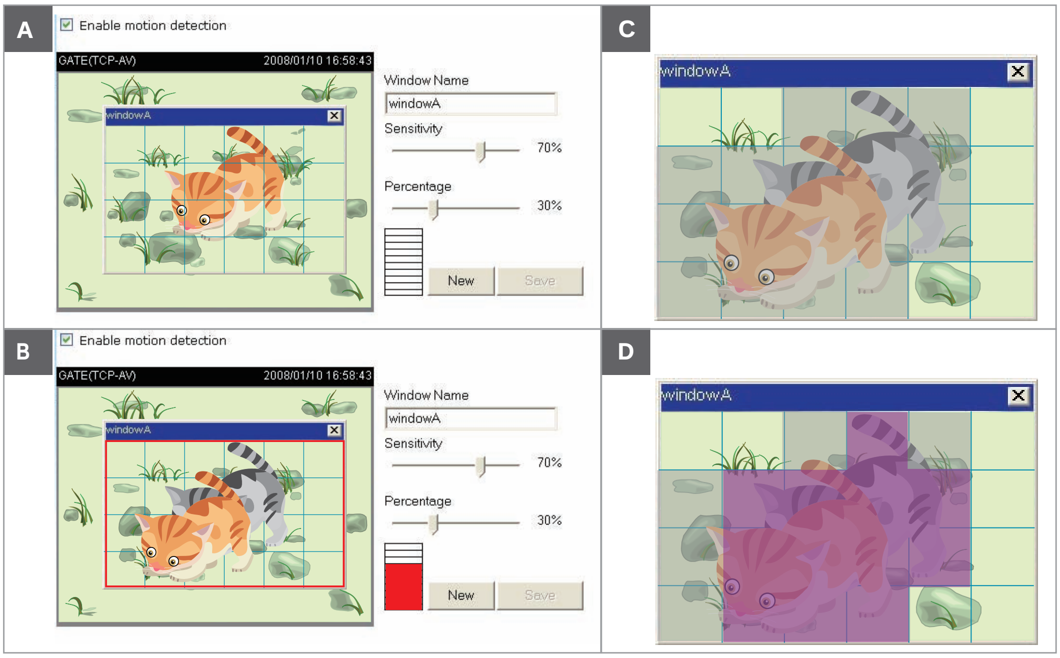
The Percentage Indicator will rise or fall depending on the image variation. When motions are detected by the Network Camera and are judged to exceed the defined threshold, a red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to send to the remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to plot an event, please refer to Application on page 46.

A green bar indicates that even though motions are detected, the event will not be triggered because the image variations are still falling under the defined threshold.



NOTE

► *How does motion detection work?*



There are two parameters for setting the motion detection: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C), and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to sense a slight movement while smaller sensitivity settings tend to neglect it. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

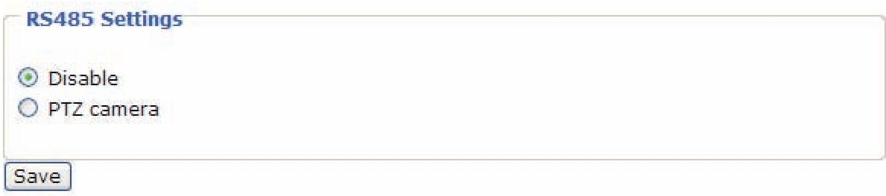
Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require higher security management, it is suggested to set higher sensitivity settings and smaller percentage values.

Camera control

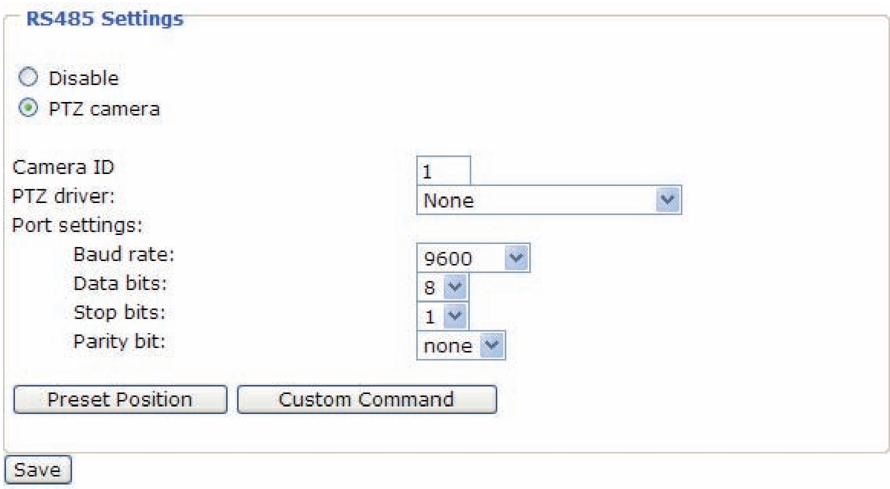
This section explains how to control the Network Camera's Pan/Tilt/Zoom operation by connecting with a PTZ driver or scanner via RS485 interface.

RS485 Settings

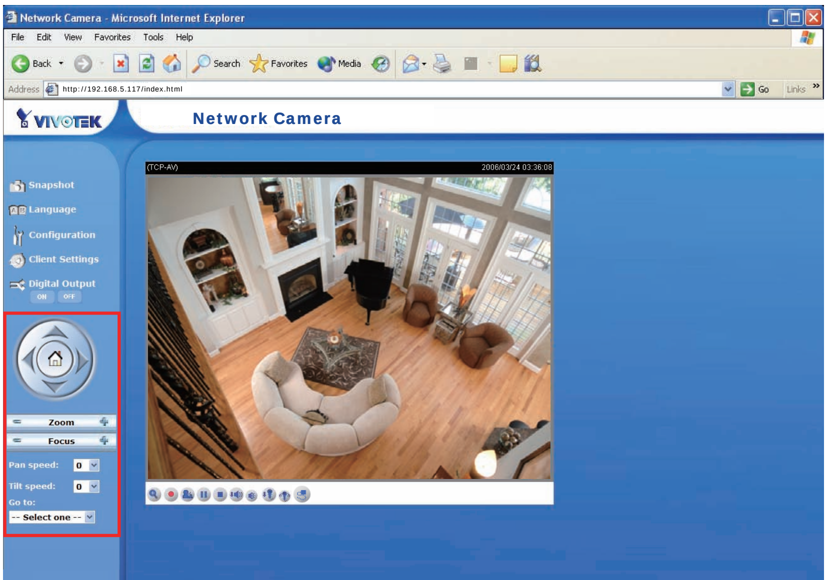


Disable: Select this option to disable this function.

PTZ camera: Select this option to enable PTZ operation.
To utilize this feature, please connect the Network Camera with a PTZ driver or scanner via RS485 interface first. And then you can configure the PTZ driver and RS485 port settings in the following diagram.



VIVOTEK offers three PTZ drivers: DynaDome/SmartDOME, Lilin PIH-7x00 and Pelco D protocol. If none of the above PTZ drivers is supported by your PTZ scanner, please select Custom camera (scanner). please refer to the user's manual of your PTZ scanner to set the Camera ID, PTZ driver, and Port settings. The Camera ID is necessary for multiple cameras control. If you select PTZ camera and click Save to enable this function, the camera control panel will be displayed in the main page as the following diagram:



Preset Position

Click Preset Position to open the Preset Position page. In this page, you can set the preset position for the Network Camera. A total of 20 preset positions can be configured.

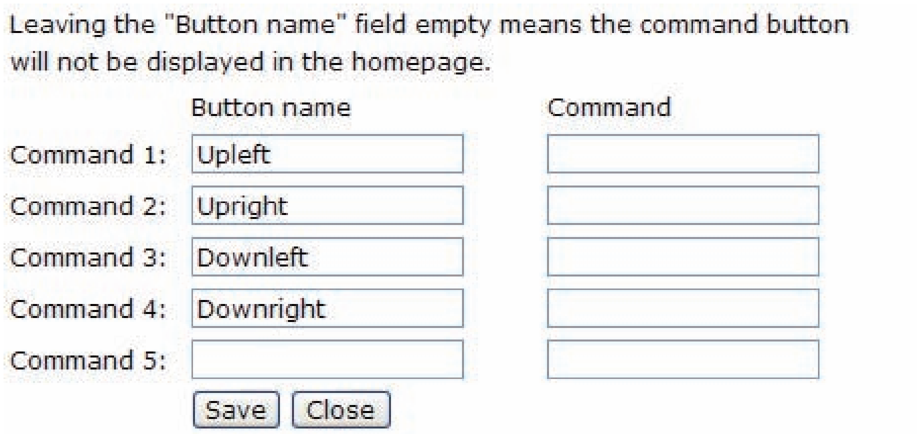


Follow the steps below to set preset positions:

1. Adjust the Network Camera to a desired position with the buttons on the right side of the window.
2. In the Preset position name text box, enter a descriptive name for the preset position. The preset position name allows up to forty characters. Click Add to take effect. The preset position name will appear in the Preset Positions drop-down list. To remove a preset position from the list, select a preset position name from the Preset Positions drop-down list and then click Delete.
3. You can click “Go to” to aim at preset positions, which will also displayed in the main page.
4. Click Save to take effect.

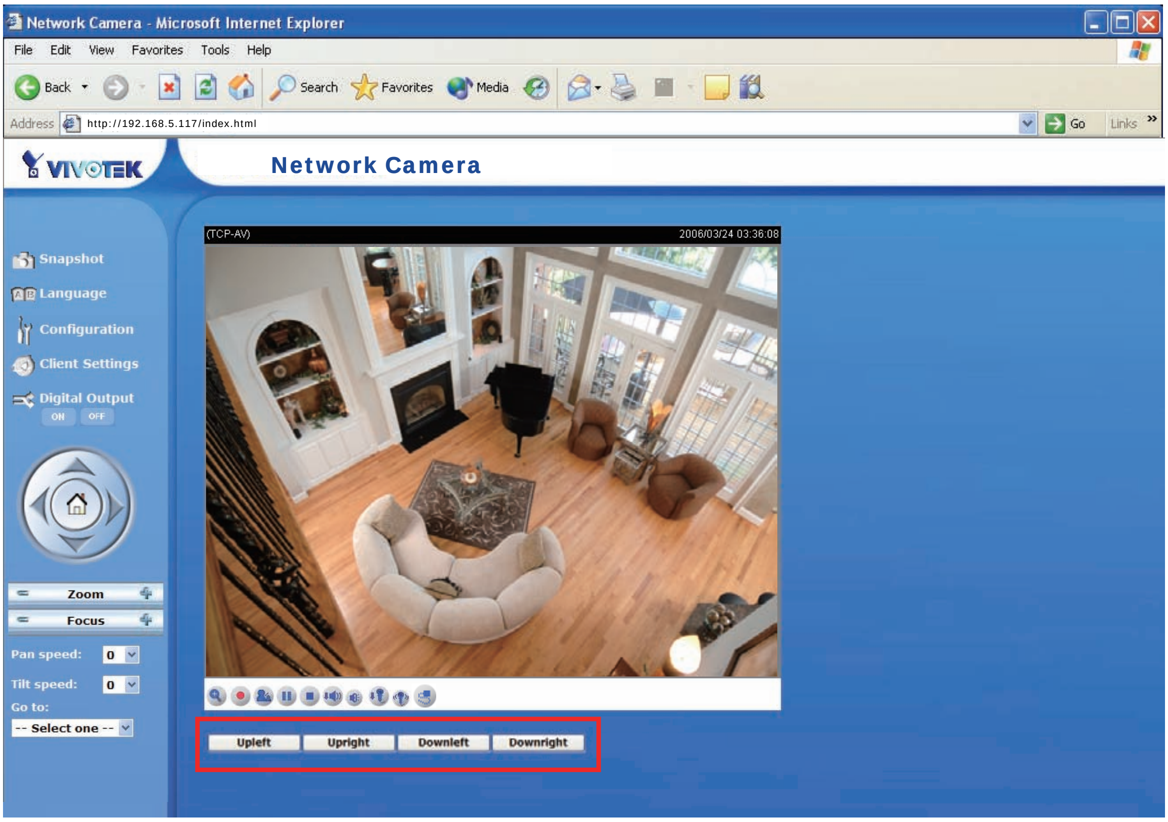
Custom Command

If the Custom camera (scanner) is selected as the PTZ driver, the PTZ control panel on the main page will not take effect. You need to **configure command buttons to control the PTZ scanner. Click Custom Command to open the Custom Command page. A total of five command buttons can be configured. Please refer to the user's manual of your PTZ scanner to enter the command in the following blanks.**



Click Save to enable the settings and click Close to quit the page.

The command button will appear in the main page as the following diagram.

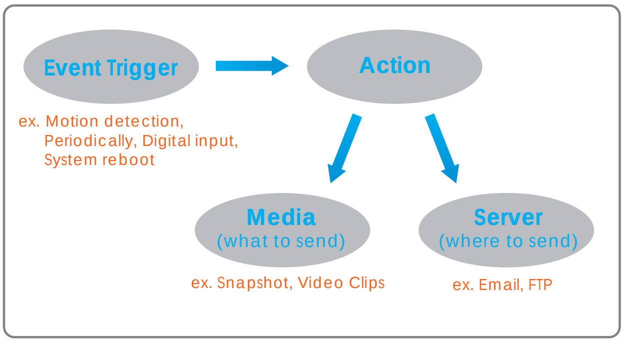


Application

This section explains how to configure the Network Camera to react in response to particular situations. A typical application is that when a motion is detected, the Network Camera sends buffered images to a FTP server or via e-mail as notifications.



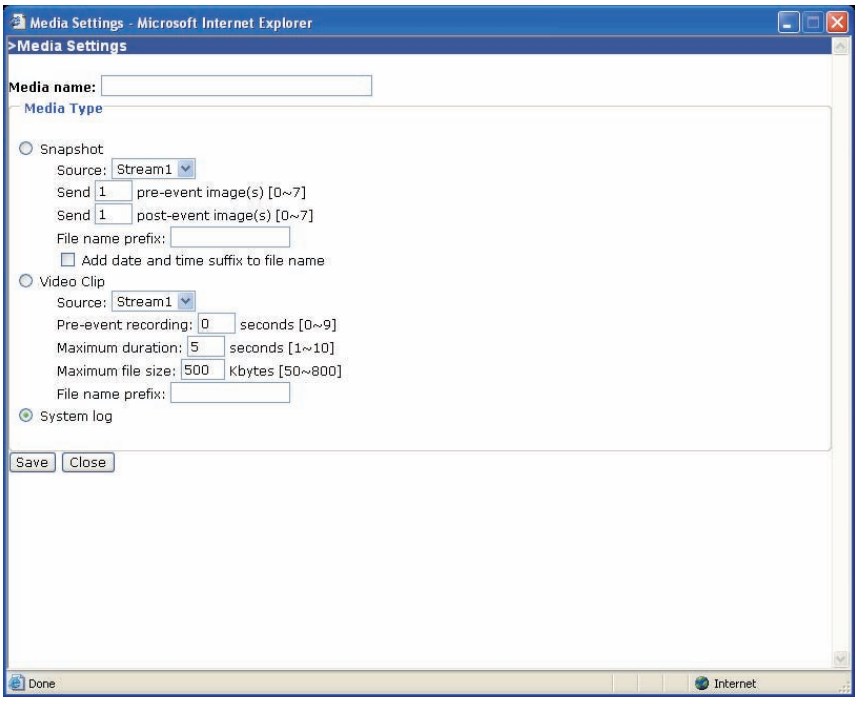
In the illustation on the right side, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what kind of action will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.



To start plotting an event, it is suggested to configure server and media columns first so that the Network Camera will know what action shall be performed when a trigger is activated.

Media Settings

In Media Settings column, click Add to open the media setting page. In this page, you can specify what kind of media to send when a trigger is activated. A total of five media settings can be configured.



Media name: Enter a descriptive name for the media setting.

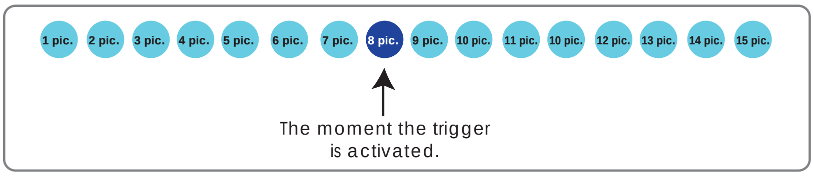
Media Type: There are three choices of media types available: Snapshot, Video Clip, and System log.

Snapshot: Select to send snapshots when a trigger is activated.

■ Source: Select to take snapshots from stream 1 or stream 2.

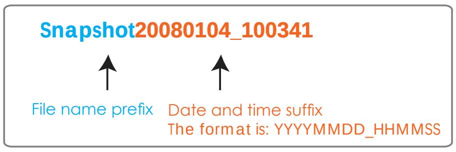
■ Send ☐ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Specify to capture how many images before a trigger is activated. Up to seven images can be generated.

■ Send ☐ post-event images
Specify to capture how many images after a trigger is activated. Up to seven images can be generated. For example, if both the Send pre-event images and Send post-event images are set to seven, a total of fifteen images are generated after a trigger is activated.

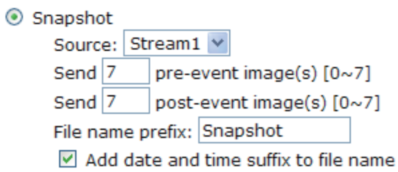


■ File Name Prefix
Enter the text that will be put in front of the file name.

■ Add date and time suffix to the file name
Select this option to add date and time to the file name suffix.



For example:

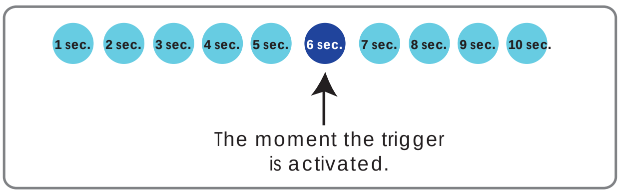


Video Clip: Select to send video clips when a trigger is activated.

■ Source: Select to record video clips from stream 1 or stream 2.

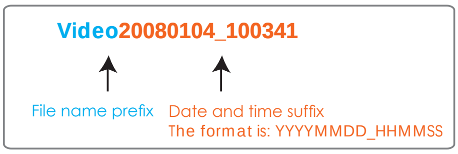
■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Specify to record video clips for how many seconds before a trigger is activated. Up to nine seconds can be set.

■ Maximum duration
Specify the maximal recording duration in seconds. Up to ten seconds can be set.
For example, if the Pre-event recording is set to five seconds and the Maximum duration is set to ten seconds, the Network Camera continues to record for another four seconds after a trigger is activated.

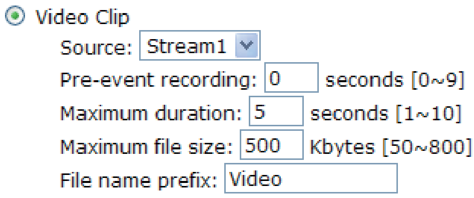


■ Maximum file size
Specify the maximal file size allowed.

■ File Name Prefix
Enter the text that will be put in front of the file name.



For example:



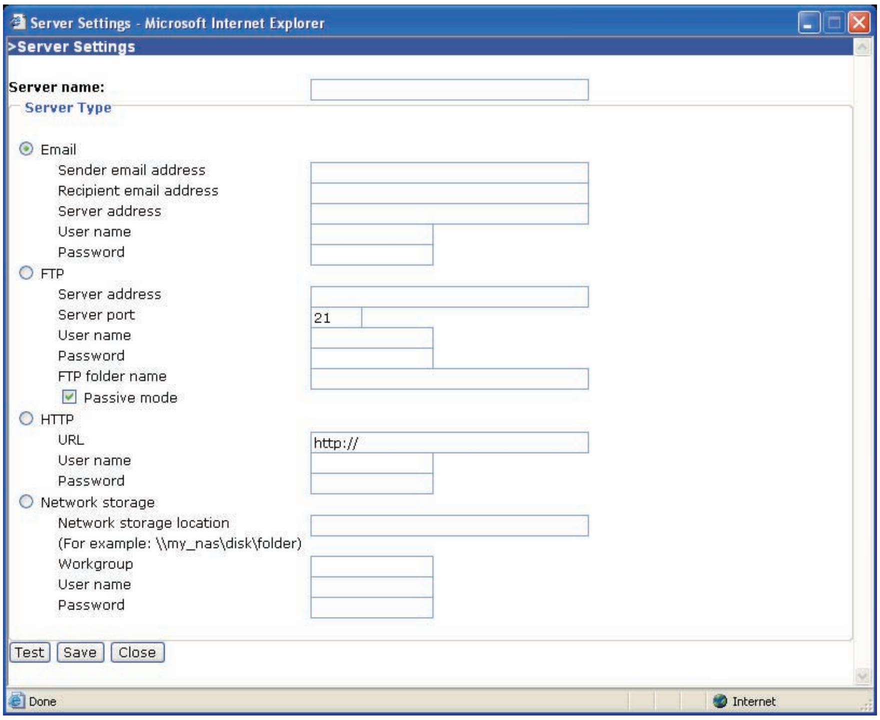
System log: Select to send a system log when a trigger is activated.

When completed, click Save to take effect and then click Close to quit this page. The new media name will appear in the media drop-down list on the Application page as below. To remove a media setting from the list, select a media name from the drop-down list and then click Delete. Note that only when the media setting is not being applied to an event setting can it be deleted.



Server Settings

In the Server column, click Add to open the server setting page. In this page, you can specify where the notification messages will be send when a trigger is activated. A total of five server settings can be configured.



Server name: Enter a descriptive name for the server setting.

Server Type: There are four choices of server types available: Email, FTP, HTTP, and Network storage.

Email: Select to send the media via Email when a trigger is activated.

■ Sender email address: Enter the email address of the sender.

■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

■ User name: Enter the user name of the email account.

■ Password: Enter the password of the email account.

To verify if the email settings are correctly configured, click Test. The result will be shown in a pop-up window. If it works, you will also receive an email indicating the result.





FTP: Select to send the media to a FTP server when a trigger is activated.

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port
By default, the FTP port server is set to 21. Also, it can be assigned with another port number between 1025 and 65535.

■ User name: Enter the login name of the FTP account.

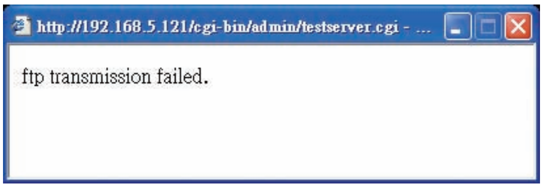
■ Password: Enter the password of the FTP account.

■ Remote folder name
Enter a folder to place the media file. If the folder name does not exist, the Network Camera will create one on the FTP server.

■ Passive Mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify if the FTP settings are correctly configured, click Test. The result will be shown in a pop-up window. If it works, you will also receive a test.txt file on the FTP server.





HTTP: Select to send the media to a HTTP server when a trigger is activated.

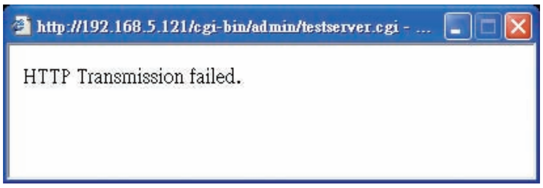
■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name.

■ Password: Enter the password.

To verify if the HTTP settings are correctly configured, click Test. The result will be shown in a pop-up window. If it works, you will also receive a test.txt file on the HTTP server.





Network storage: Select to send the media to a network storage when a trigger is activated.

■ Network storage location: Enter the path of the network storage.

■ Workgroup: Enter the workgroup for network storage.

■ User name: Enter the user name.

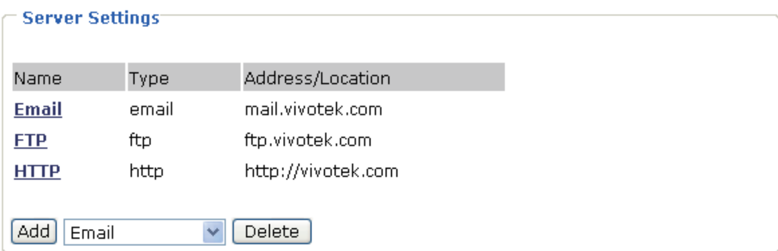
■ Password: Enter the password.

To verify if the network storage settings are correctly configured, click Test. The result will be shown in a pop-up window. If it works, you will also receive a test.txt file on the network storage server.



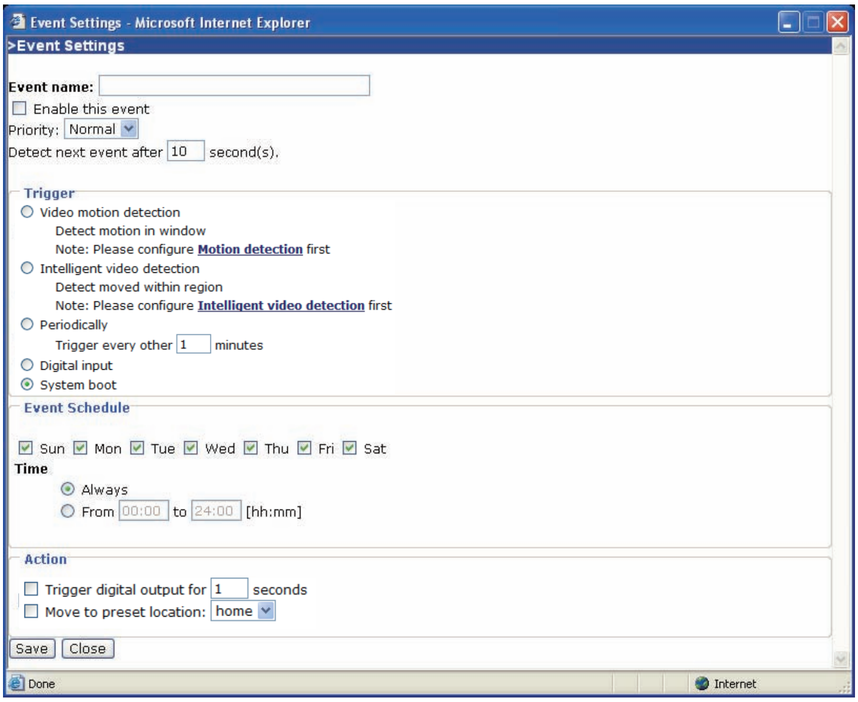


When completed, click Save to take effect and then click Close to quit this page. The new server name will appear in the server drop-down list on the application page as below. To remove a server setting from the list, select a server name from the drop-down list and then click Delete. Note that only when the server setting is not being applied to an event setting can it be deleted.



Event Settings

In the Event column, click Add to open the event setting page. In this page, you can arrange the three elements -- Trigger, Schedule and Action to plot an event. A total of three event settings can be configured.



Event name: Enter a descriptive name for the event setting.

Enable this event: Select this option to enable this event setting.

Priority: Select the relative importance of this event (High, Normal, and Low). Events with higher priority setting will be executed first.

Detect next event after ☐ seconds: Enter the duration in seconds to pause motion detection after a motion is detected.

An event is an action initiated by user-defined trigger source; it is the causal arrangement of the following three elements: Trigger, Event Schedule, and Action.

Trigger: Also referred as the cause or stimulus, defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.There are four choices of trigger sources:

■ Video motion detection
Select this option to allow the Network Camera to use the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure Motion detection first. For more information, please refer to Motion detection on page 41 for details.

■ Intelligent video detection
Select this option to allow the Network Camera to use the built-in intelligent video detection as a trigger source. To enable this function, you need to configure Video content analysis first. For more information, please refer to Video content analysis on page 55 for details.

■ Periodically
Select this option to allow the Network Camera to trigger periodically for every other defined minute. At most 999 minutes can be set.

■ Digital input
Select one of the Digital inputs to allow the Network Camera to use external digital input device as a trigger source. Depending on your applications, there are choices of digital input devices on the market which helps to sense any changes in temperature, vibration, sound and light, etc.

■ System boot
Select this option to allow the Network Camera to trigger when the power of Network Camera is disconnected.

Event Schedule: The effective period in which the event stays active. Specify the effective period for the event.

■ Select the days on weekly basis.

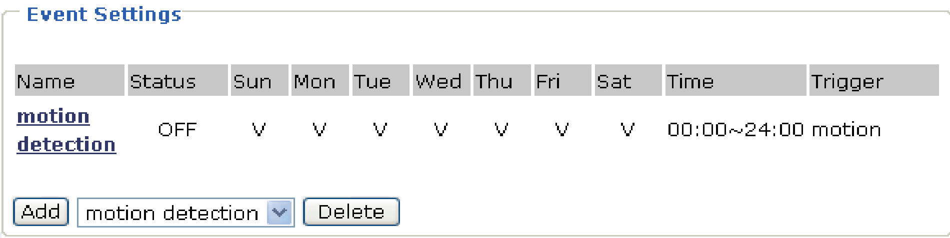
■ Select the time for recording in 24-hr time format.

Action: Also referred as the effect, defines the action to be performed by the Network Camera when the trigger is activated. Select the action to perfom when a trigger is activated.

■ Trigger D/O for ☐ seconds
Select this option to turn on external digital output device when a trigger is activated. Specify the length of trigger interval in the text box.

■ Server name / Media name
Select the server and media name to allow the Network Camera to send the media files to the server when a trigger is activated.

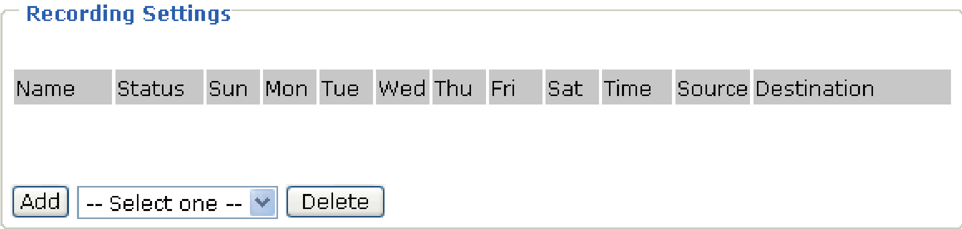
When completed, select Enable this event. Click Save to take effect and then click Close to quit this page. The new event name will appear in the event drop-down list on the application page. To remove an event setting from the list, select an event name from the drop-down list and then click Delete.



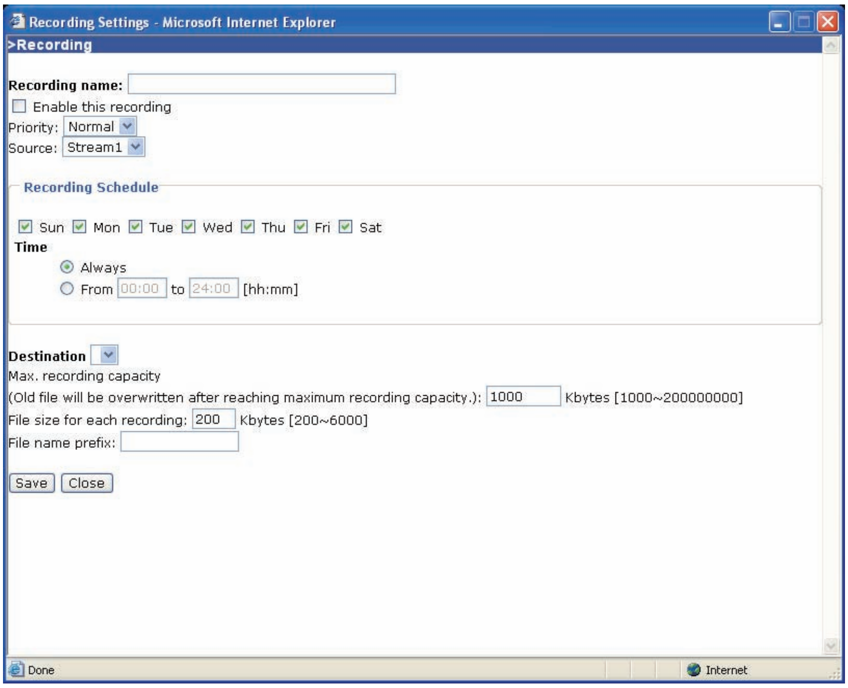
Recording

This section explains how to configure the recording settings for the Network Camera.

Recording Settings



Click Add to open the recording setting page. In this page, you can define the recording source, recording schedule and recording capacity. A total of two recording settings can be configured.



<u>Recording name</u>: Enter a descriptive name for the recording setting.

<u>Enable this recording</u>: Select this option to enable video recording.

<u>Priority</u>: Select the relative importance of this recording setting (High, Normal, and Low).

<u>Source</u>: Select the recording source (stream 1 or stream 2).

<u>Recording Schedule</u>: Specify the recording duration.

■ Select the days on weekly basis.

■ Select the time for recording in 24-hr time format.

Destination: Specify a storage destination for the recorded video files. Note that the destination field is empty by default. Please go to Configuration > Application > Server Settings to set a Network storage server; please refer to Server Settings on page 48.

Max. recording capacity: Please note that when the maximum capacity is reached, the oldest file will be overwritten by the latest one.

File size for each recording: Specify the file size for each recording media.

File name prefix: Enter the text that will be put in front of the file name.

When completed, select Enable this recording. Click Save to take effect and then click Close to quit this page. The new recording name will appear in the recording drop-down list on the recording page. To remove a recording setting from the list, select a recording name from the drop-down list then and click Delete.



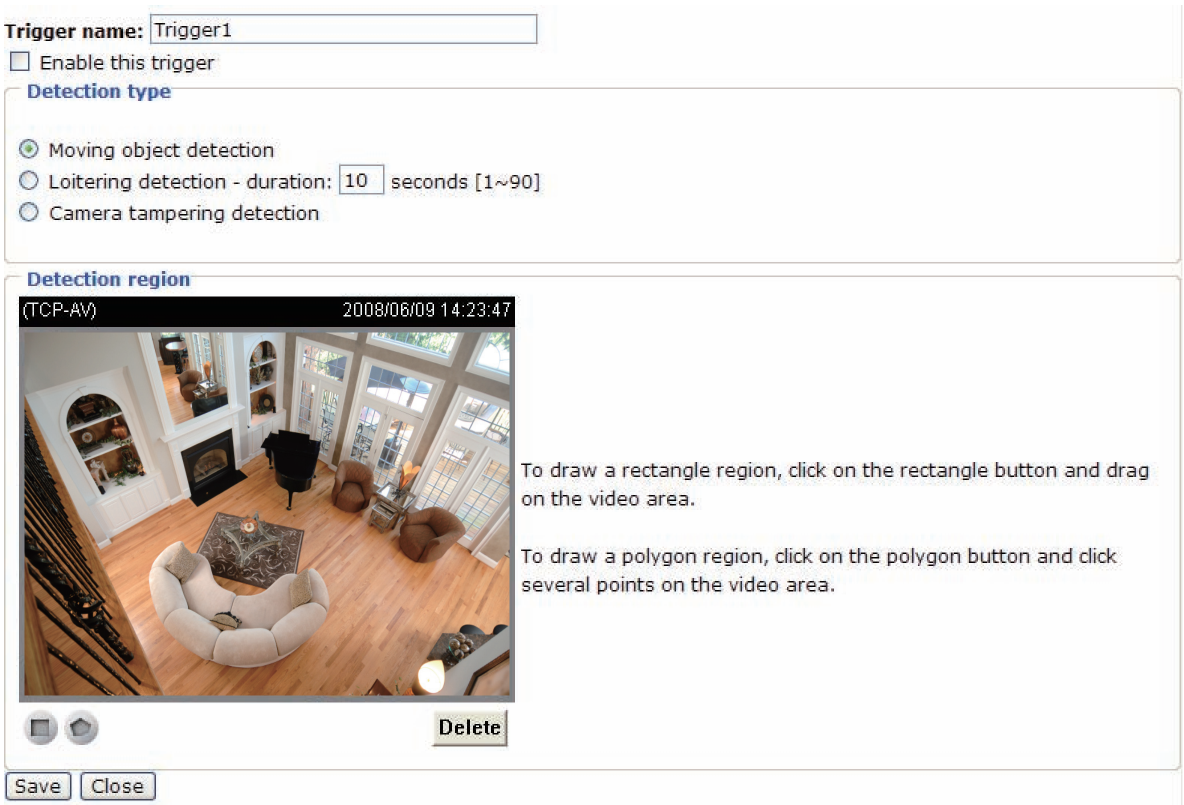
Video content analysis

This section explains how to configure the video content analysis function for the Network Camera. Incorporating a powerful digital signal processor (DSP) dedicated to the video content analysis, it features three reliable and helpful detections including moving object detection, and loitering detection, and tampering detection.
The embedded video content analysis, superior to conventional motion detection function, is capable of distinguishing between creature's motions and still backgrounds or natural movements like swaying trees, waves or sunset so as to prevent the false alarms from environmental noise. In addition, with the tampering detection, it also can detect incidents such as shooting redirection, blocking or defocusing of cameras, or even spray-painted.

Trigger

Name	Status
Trigger1	OFF
Trigger2	OFF
Trigger3	OFF

Click Trigger1 to open the trigger setting page. In this page, you can define the detection type and detection region. A total of three trigger settings can be configured.



Trigger name: Enter a descriptive name for the recording setting.

Enable this trigger: Select this option to enable this trigger.

Detection type: Select one of the following detection types as the trigger source.

■ Moving object detection: Select this option to track the path of moving object.

■ Loitering detection - duration: □seconds [1~90]
Select this option to detect a suspicious object in the predefined area (window) for a long period of

time. It will trigger the alarm once the dwelling time of the object is longer than the given time.

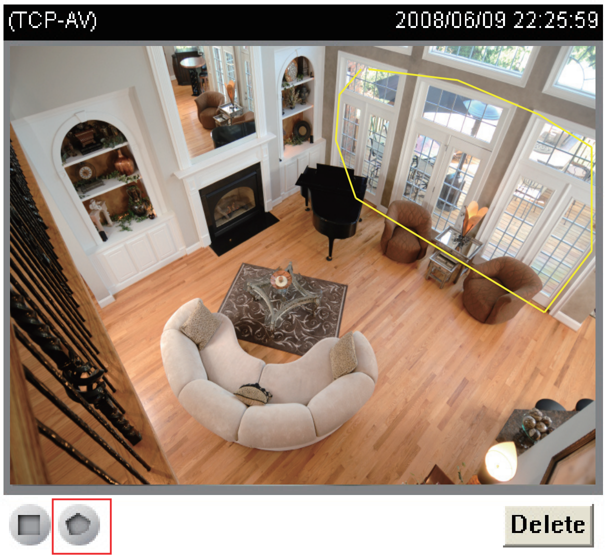
■ Camera tampering detection: Select this option to detect camera tampering.

Detection region: Draw a detection region.

■ To draw a rectangle region, click on the rectangle button to entering the drawing mode. The button will becomes and you can click and drag to draw a rectangle on the video area as the left diagram below.

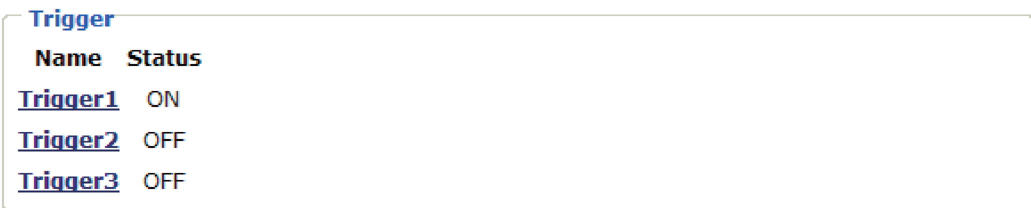
■ To draw a polygon region, click on the polygon button to entering the drawing mode. The button will becomes and you and click several points on the video area to link a polygon region. Note that the maximum number of points of the polynomial should be 10.





Note that you can only draw either a rectangle region or a polygon region. The buttons will turn to which can not be configured.

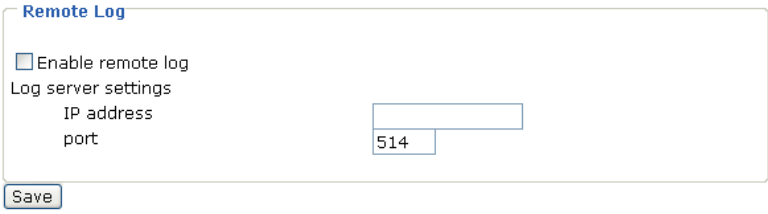
You can click Delete to erase the detection region. When completed, select Enable this trigger. Click Save to take effect and then click Close to quit this page.
The status of trigger will turn to “ON“ on the Video content analysis page as below.



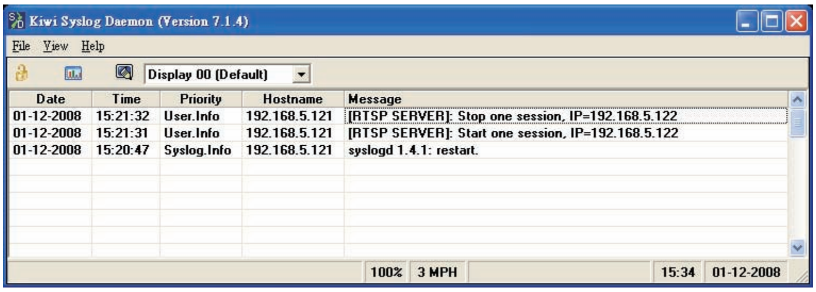
System log

This section explains how to configure the Network Camera to send system log to remote server as a backup. It is composed of the following two columns: Remote Log and Current Log.

Remote Log



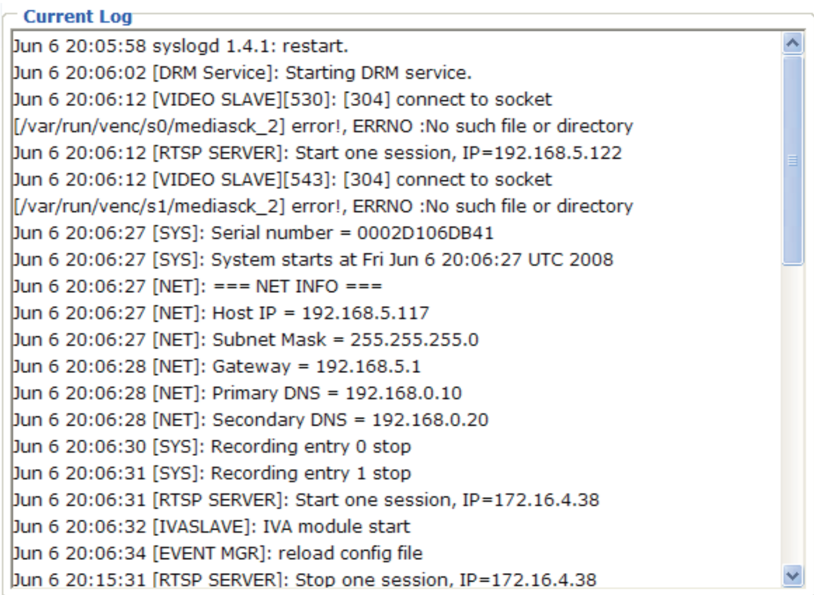
You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested to install a log-recording tool to receive system log messages from the Network Camera. For example, a tool -- Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.



Follow the steps below to set up the remote log:

1. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, select Enable remote log and click Save to take effect.

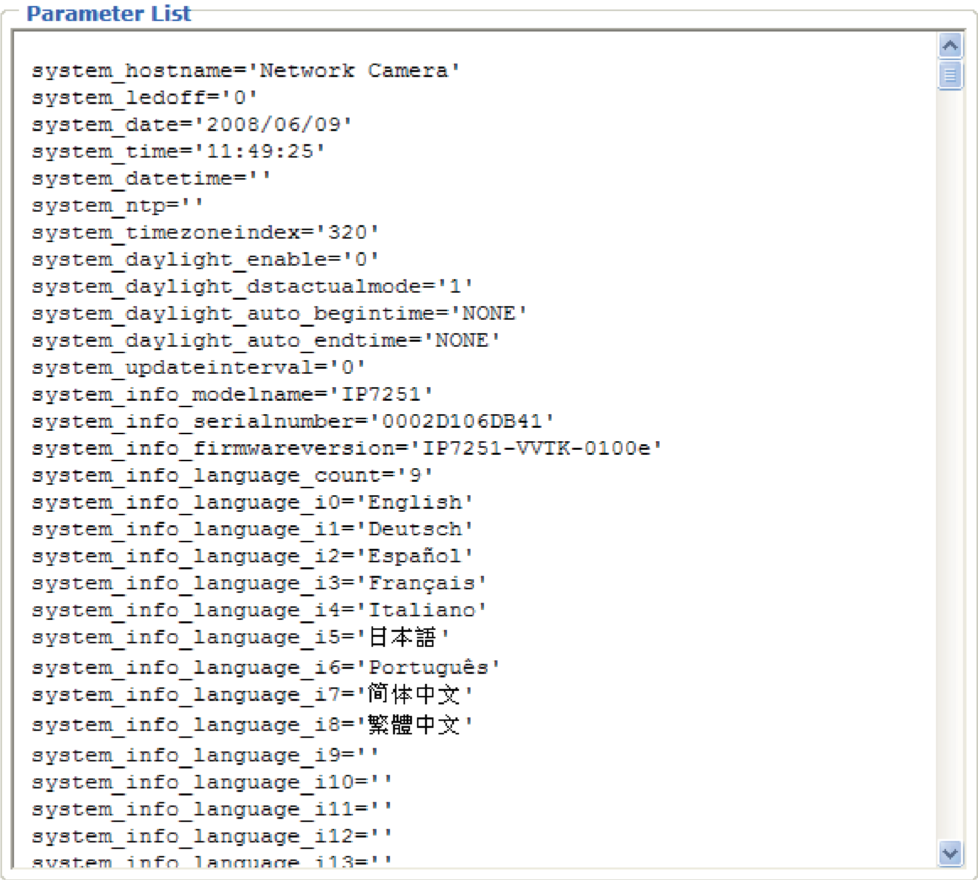
Current Log



This column displays the system's log in chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain amount.

View parameters

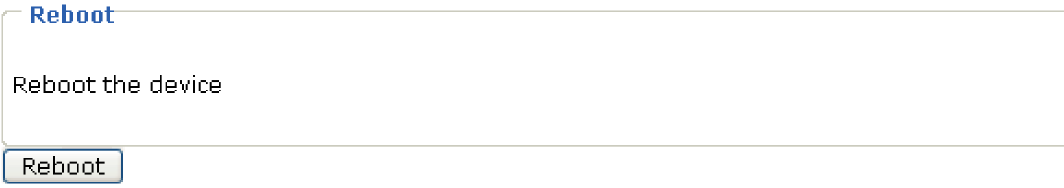
The View parameters page lists the entire system’s parameters in alphabetical order. If you need technical assistance, please provide the information listed in this page.



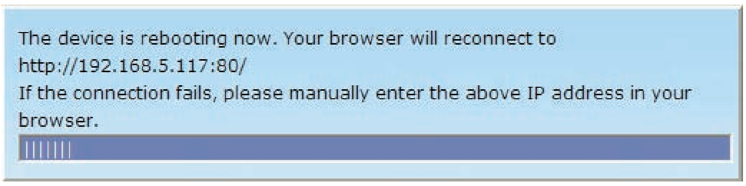
Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

Reboot

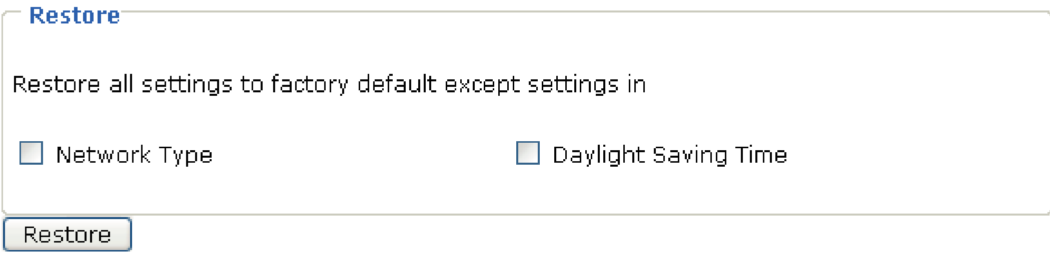


This feature allows you to turn off and then turn on the Network Camera. It takes about one ~ two minutes to complete the process. When completed, the live video will be displayed in your browser. The following message is displayed during the rebooting process.



If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

Restore



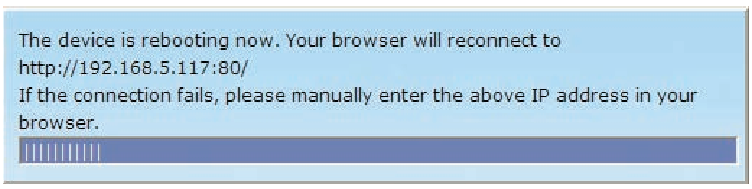
This feature allows you to restore the Network Camera to factory default. Two settings can be excluded:

<u>Network Type</u>: Select this option to retain the Network Type settings (please refer to Network Type on page 24).

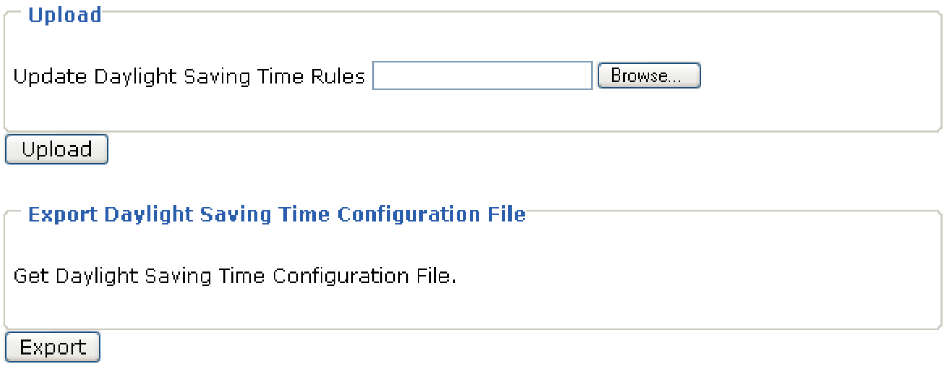
<u>Daylight Saving Time</u>: Select this option to retain the Daylight Saving Time settings (please refer to System on page 21).

If none of the options is selected, all settings will be restored to factory default.

The following message is displayed during the restoring process.

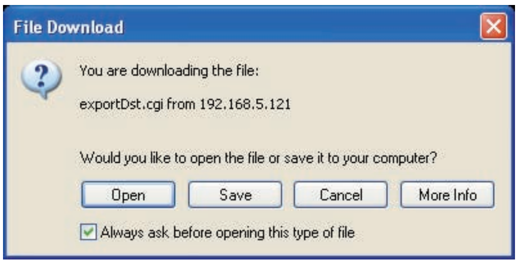


Upload / Export Daylight Saving Time Configuration File

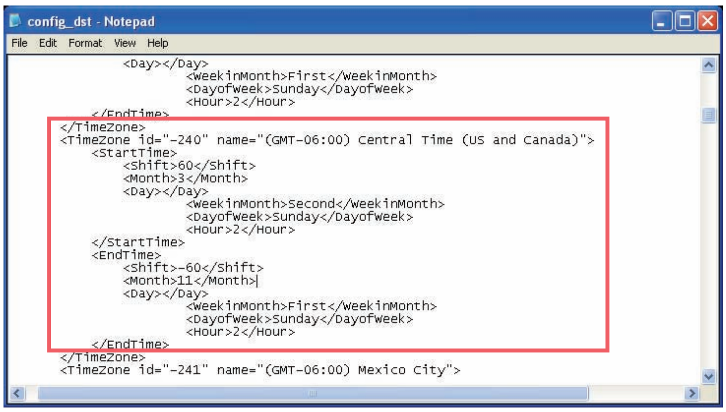


This feature allows you to set the starting time and ending time of DST.
Follow the steps below to set up:

1. In the Export Daylight Saving Time Configuration File Column, click Export to export an Extensible Markup Language (*.xml) file from the Network Camera.
2. Open the XML file using Microsoft® Notepad and locate your time zone; set the starting time and ending time of the DST. When completed, save the file.

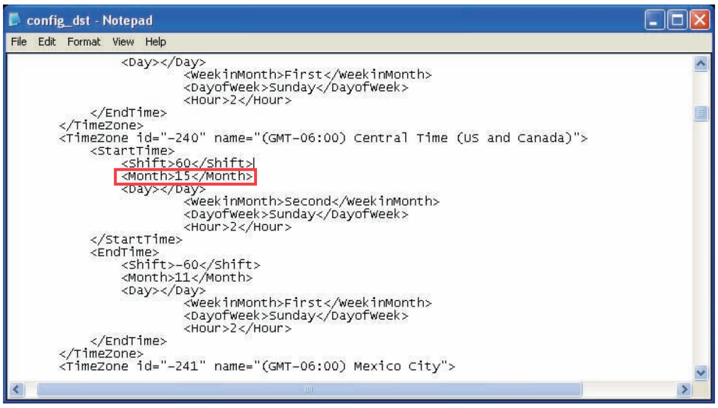


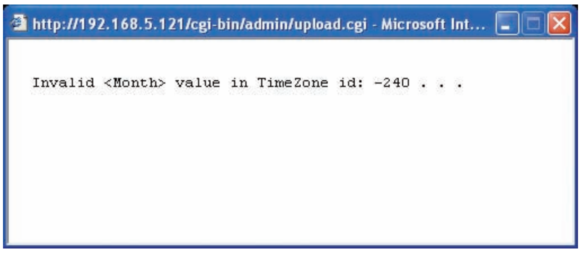
In the example below, the DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



3. In the Upload Column, click Browse… and specify the XML file.

If the incorrect date and time is assigned, you will see the following warning message when uploading the file to the Network Camera.

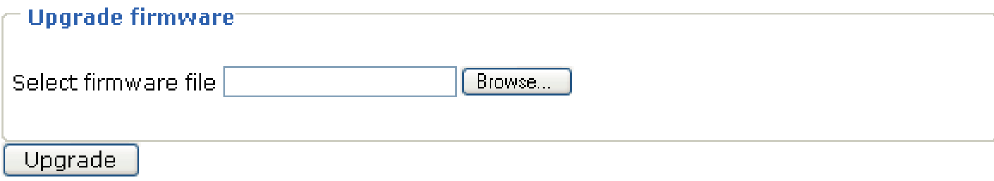




4. Click Upload. To enable the DST, see System Time on page 22.
The following message is displayed when attempting to upload an incorrect file format.



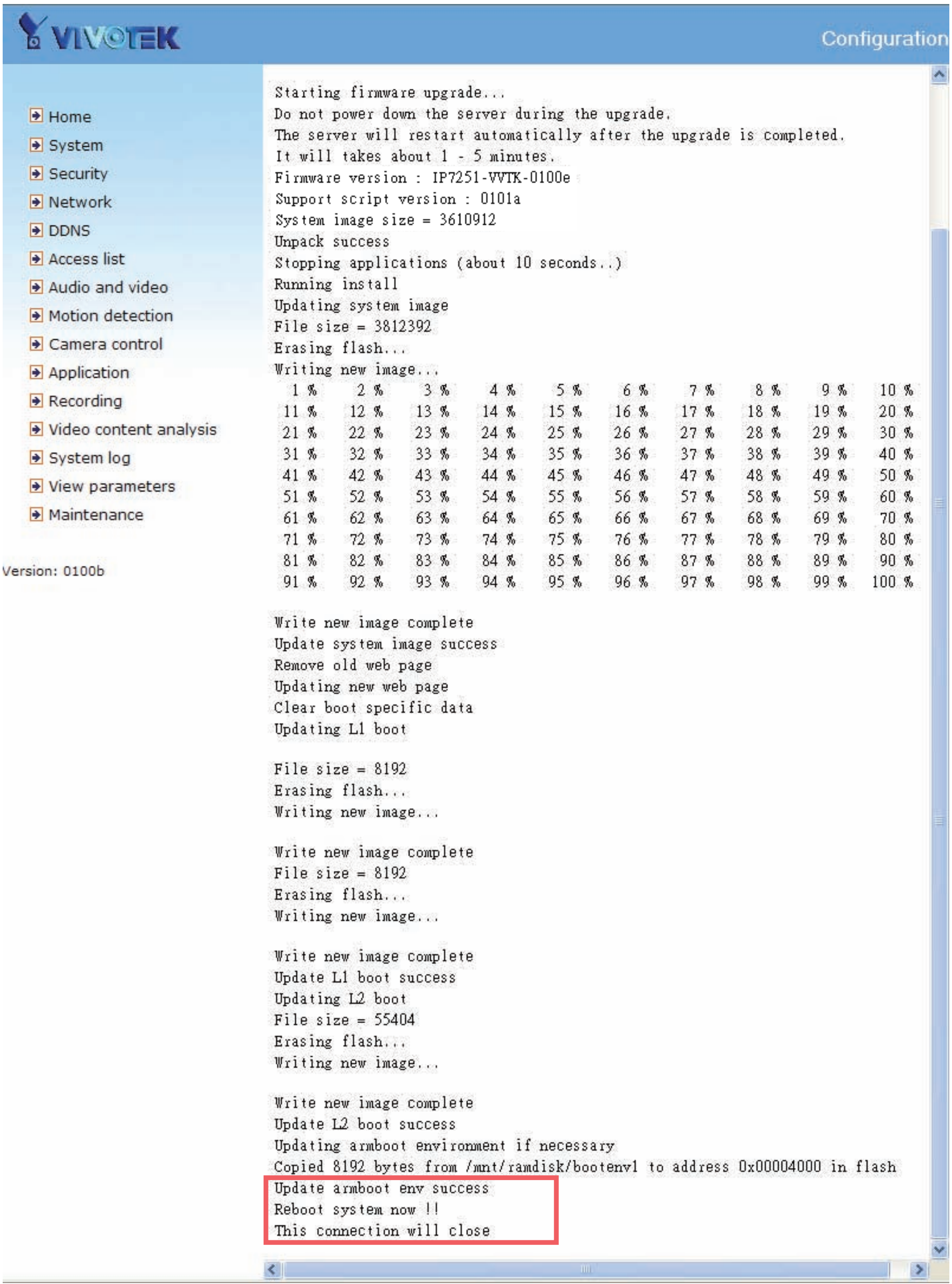
Upgrade Firmware



This feature allows you to upgrade the firmware on your Network Camera. It takes about five minutes to complete the process.
Note that do not power off the Network Camera during the upgrade.

Follow the steps below to upgrade firmware:
1. Download a new firmware file from VIVOTEK website. The file is in pkg file format.
2. Click Browse… and specify the firmware file.
3. Click Upgrade. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

The upgrade is successful as you see "Reboot system now!! This connection will close". After that, re-access the Network Camera.
The following message is displayed when the upgrade is succeeded.



The following message is displayed when you have selected an incorrect firmware file.

Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is completed.
It will takes about 1 - 5 minutes.
Wrong PKG file format
Unpack fail

Appendix

URL Commands of the Network Camera

Overview

For some customers who already have their own web site or web control application, Network Camera/ Video server can be easily integrated through convenient URLs. This section specifies the external HTTP based application programming interface. The HTTP based camera interface provides the functionality to request a single image, to control camera functions (PTZ, output relay etc.) and to get and set internal parameter values. The image and CGI-requests are handled by the built in Web server.

Style convention

In URL syntax and in descriptions of CGI parameters, a text within angle brackets denotes a content that is to be replaced with either a value or a string. When replacing the text string also the angle brackets shall be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example, also below.

URL syntax' are written with the “**Syntax:**" word written in bold face followed by a box with the referred syntax as seen below. The name of the server is written as <servername>. This is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam. adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data returned as HTTP formatted, i.e., starting with the string HTTP is line separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

General CGI URL syntax and parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, the internal parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in function related directories under the cgi-bin directory. The file extension of the CGI is required.

Syntax:

```
http://<servername>/cgi-bin/<subdir>[/<subdir>...]/<cgi>.<ext>
[?<parameter>=<value>[&<parameter>=<value>...]]
```

Example: Setting digital output #1 to active

```
http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1
```

Security level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera 2. Can control dido, ptz of camera
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator's access right can modify most of camera's parameters except some privilege and network options
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator's access right can fully control the camera's operation.
7	N/A	Internal parameters. Unable to be changed by any external interface.

Get server parameter values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/getparam.cgi?[<parameter>]
[&<parameter>...]
```

```
http://<servername>/cgi-bin/viewer/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/operator/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/admin/getparam.cgi?[<parameter>]
[&<parameter>…]
```

where the *<parameter>* should be *<group>*[_*<name>*] or *<group>*[.*<name>*] If you do not specify the any parameters, all the parameters on the server will be returned. If you specify only *<group>*, the parameters of related group will be returned.

When query parameter values, the current parameter value are returned.

Successful control request returns paramter pairs as follows.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

<length> is the actual length of content.

Example: request IP address and it's response

```
Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Set server parameter values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>...][&update=<value>][&return=<return page>]

http://<servername>/cgi-bin/viewer/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>...][&update=<value>] [&return=<return page>]

http://<servername>/cgi-bin/operator/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>...][&update=<value>] [&return=<return page>]

http://<servername>/cgi-bin/admin/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>...][&update=<value>] [&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign <*value*> to the parameter <*group*>_<*name*>
update	<boolean>	set to 1 to actually update all fields (no need to use update parameter in each group)
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page. (note: The return page can be a general HTML file(.htm, .html) or a Vivotek server script executable (.vspx) file. It can not be a CGI command. It can not have any extra parameters. This parameter must be put at end of parameter list)

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
```

<parameter pair>

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and readable will be returned.

Example: Set the IP address of server to 192.168.0.123

Request:

http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Context-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

Available parameters on the server

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text string shorter than 'n' characters. The characters ",', <,>,& are invalid.
password[<n>]	The same as string but display '*' instead
integer	Any number between (-2^{31} – 1) and (2^{31} – 1)
positive integer	Any number between 0 and (2^{32} – 1)
<m> ~ <n>	Any number between 'm' and 'n'
domain name[<n>]	A string limited to contain a domain name shorter than 'n' characters (eg. www.ibm.com)
email address [<n>]	A string limited to contain a email address shorter than 'n' characters (eg. joe@www.ibm.com)
ip address	A string limited to contain an ip address (eg. 192.168.1.1)
mac address	A string limited to contain mac address without hyphen or colon connected
boolean	A boolean value 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>,	Enumeration. Only given values are valid.

...	
blank	A blank string
everything inside < >	As description

NOTE: The camera should prevent to restart when parameter changed.

Group: **system**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	IP7251 Network Camera	1/6	host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server)
ledoff	<boolean>	0	6/6	turn on(0) or turn off(1) all led indicators
date	<yyyy/mm/dd>, keep, auto	<current date>	6/6	Current date of system. Set to ‘keep’ keeping date unchanged. Set to ‘auto’ to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	<current time>	6/6	Current time of system. Set to ‘keep’ keeping time unchanged. Set to ‘auto’ to use NTP to synchronize time.
ntp	<domain name>, <ip address>, <blank>	<blank>	6/6	NTP server *do not use “skip to invoke default server” for default
timezoneindex	-480 ~ 520	320	6/6	Indicate timezone and area -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las

				Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -160: GMT-04:00 Atlantic Time, Canada, Caracas ,La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Time:Dublin, Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo

				82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide,

				Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean>	0	6/6	enable automatic daylight saving to time zone
daylight_dstactualmode	<boolean>	1	6/7	check if current time is under daylight saving time.
daylight_auto_begintime	string[19]	NONE	6/7	display the current daylight saving begin time. (product dependent)
daylight_auto_endtime	string[19]	NONE	6/7	display the current daylight saving end time. (product dependent)
updateinterval	0, 3600, 86400, 604800, 2592000	0	6/6	0 to Disable automatic time adjustment, otherwise, it means the seconds between NTP automatic update interval.
restore	0, <positive integer>	N/A	7/6	Restore the system parameters to default value after <value> seconds.
reset	0, <positive integer>	N/A	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	N/A	7/6	Restore the system

				parameters to default value except (ipaddress, subnet, router, dns1, dns2, pppoe).
restoreexceptdst	<Any value>	N/A	7/6	Restore the system parameters to default value except all daylight saving time settings.

SubGroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	IP7251	0/7	Internal model name of server (eg. IP7139)
extendedmodelname	string[40]	IP7251	0/7	ODM specific model name of server (eg. DCS-5610). If it is not ODM case, this field will be equal to “modelname”
serialnumber	<mac address>	<product mac address>	0/7	12 characters mac address without hyphen connected
firmwareversion	string[40]	<product dependent>	0/7	The version of firmware, including model, company, and version number in the format <MODEL-BRAND-VERSION>
language_count	<integer>	9	0/7	number of webpage language available on the server
language_i<0~(count-1)>	string[16]	<product dependent>	0/7	Available language lists

Group: **status**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered
do_i<0~ndi-1)>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered
onlinenum_rtsp	integer	0	6/7	current RTSP connection

				numbers
onlinenum_sip	integer	0	6/7	current SIP connection numbers
onlinenum_httppush	integer	0	6/7	current HTTP push server connection numbers

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	high	1/1	indicate whether open circuit or closed circuit represents inactive status

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	open	1/1	indicate whether open circuit or closed circuit represents inactive status

Group: security

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
user_i0_name	string[64]	root	6/7	User's name of root
user_i<1~20>_name	string[64]	<blank>	6/7	User's name
user_i0_pass	password[64]	<blank>	6/6	root's password
user_i<1~20>_pass	password[64]	<blank>	7/6	User's password
user_i0_privilege	viewer, operator, admin	admin	6/7	root's privilege
user_i<1~20>_ privilege	viewer, operator, admin	viewer	6/6	User's privilege.

Group: **network**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
type	lan, pppoe	lan	6/6	Network connection type

resetip	<boolean>	1	6/6	1 => get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot 0 => use preset ipaddress, subnet, rounter, dns1, and dns2
ipaddress	<ip address>	<product dependent>	6/6	IP address of server
subnet	<ip address>	<blank>	6/6	subnet mask
router	<ip address>	<blank>	6/6	default gateway
dns1	<ip address>	<blank>	6/6	primary DNS server
dns2	<ip address>	<blank>	6/6	secondary DNS server
wins1	<ip address>	<blank>	6/6	primary WINS server
wins2	<ip address>	<blank>	6/6	secondary WINS server

Subgroup of **network**: **ftp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	21	6/6	local ftp server port

Subgroup of **network**: **http**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	80	6/6	HTTP port
alternateport	1025~65535	8080	6/6	Alternative HTTP port
authmode	basic, digest	basic	1/6	HTTP authentication mode
s0_accessname	string[32]	video.mjpg	1/6	Http server push access name for stream 1 (capability.protocol.spush_mjpeg =1 and video.stream.count>0)
s1_accessname	string[32]	video2.mjpg	1/6	Http server push access name for stream 2 (capability.protocol.spush_mjpeg =1 and video.stream.count>1)

Subgroup of **network**: **rtsp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION

port	554, 1025 ~ 65535	554	1/6	RTSP port (capability.protocol.rtsp=1)
authmode	disable, basic, digest	disable	1/6	RTSP authentication mode (capability.protocol.rtsp=1)
s0_accessname	string[32]	live.sdp	1/6	RTSP access name for stream1 (capability.protocol.rtsp=1 and video.stream.count>0)
s1_accessname	string[32]	live2.sdp	1/6	RTSP access name for stream2 (capability.protocol.rtsp=1 and video.stream.count>1)
s0_audiotrack	<integer>	0	6/6	The current audio track for stream1. -1 => audio mute
s1_audiotrack	<integer>	0	6/6	The current audio track for stream2. -1 => audio mute

Subgroup of **rtsp_s<0~(n-1)>**: **multicast,** n is stream count (capability.protocol.rtp.multicast=1)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	0	4/4	Enable always multicast
ipaddress	<ip address>	For n=0, 239.128.1.99 For n=1, 239.128.1.100, and so on.	4/4	Multicast IP address
videoport	1025 ~ 65535	5560+n*2	4/4	Multicast video port
audioport	1025 ~ 65535	5562+n*2	4/4	Multicast audio port
ttl	1 ~ 255	15	4/4	Mutlicast time to live value

Subgroup of **network**: **sip**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65535	5060	6/6	SIP port

				(capability.protocol.sip=1)

Subgroup of **network**: **rtp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	5556	6/6	video channel port for RTP (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	5558	6/6	audio channel port for RTP (capability.protocol.rtp_unicast=1)

Subgroup of **network**: **pppoe**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
user	string[128]	<blank>	6/6	PPPoE account user name
pass	password[64]	<blank>	6/6	PPPoE account password

Group: ipfilter

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
allow_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	allow_0_start => 1.0.0.0 allow_<1~9>_start => <blank>	6/6	Allowed starting IP address for RTSP connection
allow_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	allow_0_end => 255.255.255.255 allow_<1~9>_end => <blank>	6/6	Allowed ending IP address for RTSP connection
deny_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	<blank>	6/6	Denied starting IP address for RTSP connection
deny_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	<blank>	6/6	Denied ending IP address for RTSP connection

Group: **videoin**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	60	4/4	CMOS frequency (videoin.type=2) (product dependent)
whitebalance	auto, indoor, fluorescent, outdoor	auto	4/4	auto, indoor, fluorescent, outdoor
enableblc	<boolean>	0	4/4	Enable backlight compensation (product dependent)
agc	normal, max	max	4/4	Set auto gain control to normal level or MAX level (product dependent)

Group: **videoin_c<0~(n-1)>** for n channel products, m is stream number

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
color	0, 1	1	4/4	0 =>monochrome 1 => color
flip	<boolean>	0	4/4	flip the image
mirror	<boolean>	0	4/4	mirror the image
ptzstatus	<integer>	2	1/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => Support camera control function 0(not support), 1(support) Bit 1 => **Build-in** or **external** camera. 0(external), 1(build-in) Bit 2 => Support **pan** operation. 0(not support), 1(support) Bit 3 => Support **tilt** operation. 0(not

				support), 1(support) Bit 4 => Support **zoom** operation. 0(not support), 1(support) Bit 5 => Support **focus** operation. 0(not support), 1(support)
text	string[16]	<blank>	1/4	enclosed caption
imprinttimestamp	<boolean>	0	4/4	Overlay time stamp on video
maxexposure	1~120	5	4/4	Maximum exposure time
s<0~(m-1)>_codectype	mpeg4, mjpeg	mpeg4	4/4	video codec type
s<0~(m-1)>_resolution	VGA CMOS => 176x144, 320x240, 640x480	CMOS => 640x480	4/4	Video resolution in pixel
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	The period of intra frame in milliseconds
s<0~(m-1)>_mpeg4_ratecontrol mode	cbr, vbr	vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	1, 2, 3, 4, 5	3	4/4	quality of video when choosing vbr in "ratecontrolmode". 1 is worst quality and 5 is the best quality.
s<0~(m-1)>_mpeg4_bitrate	20000, 30000, 40000, 50000, 64000, 128000, 256000, 512000, 768000,	512000	4/4	set bit rate in bps when choose cbr in "ratecontrolmode"

	1000000, 1200000, 1500000, 2000000, 3000000, 4000000			
s<0~(m-1)>_mpeg4_maxframe	1, 2, 3, 5, 10, 15, 20, 25, 30 (only for NTSC or 60Hz CMOS)	25 => PAL CCD or 50Hz CMOS 30 => NTSC CCD or 60Hz CMOS	4/4	set maximum frame rate in fps (for MPEG-4)
s<0~(m-1)>_mjpeg_quant	1, 2, 3, 4, 5	3	4/4	quality of jpeg video. 1 is worst quality and 5 is the best quality.
s<0~(m-1)>_mjpeg_maxframe	1, 2, 3, 5, 10, 15, 20, 25, 30 (only for NTSC or 60Hz CMOS)	25 => PAL CCD or 50Hz CMOS 30 => NTSC CCD or 60Hz CMOS	4/4	set maximum frame rate in fps (for JPEG)

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
source	micin, linein	linein	4/4	micin => use external microphone input linein => use line input
mute	0, 1	0	4/4	Enable audio mute
gain	0~31	0	4/4	Gain of input
boostmic	0, 1	0	4/4	Enable microphone boost
s<0~(m-1)>_codectype	aac4, gamr	gamr	4/4	set audio codec type for input

s<0~(m-1)>_aac4_bitrate	16000, 32000, 48000, 64000, 96000, 128000	128000	4/4	set AAC4 bitrate in bps
s<0~(m-1)>_gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	12200	4/4	set AMR bitrate in bps

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5	0	4/4	Adjust brightness of image according to mode settings.
saturation	-5 ~ 5	0	4/4	Adjust saturation of image according to mode settings.
contrast	-5 ~ 5	0	4/4	Adjust contrast of image according to mode settings.
sharpness	-3 ~ 3	3	4/4	Adjust sharpness of image according to mode settings.

Group: **imagepreview_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5	0	4/4	Preview of adjusting brightness of image according to mode settings.
saturation	-5 ~ 5	0	4/4	Preview of adjusting saturation of image according to mode settings.
contrast	-5 ~ 5	0	4/4	Preview of adjusting

				contrast of image according to mode settings.
sharpness	-3 ~ 3	3	4/4	Preview of adjusting sharpness of image according to mode settings.

Group: **motion_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	enable motion detection
win_i<0~2>_enable	<boolean>	0	4/4	enable motion window 1~3
win_i <0~2>_name	string[14]	<blank>	4/4	name of motion window 1~3
win_i <0~2>_left	0 ~ 320	0	4/4	Left coordinate of window position.
win_i <0~2>_top	0 ~ 240	0	4/4	Top coordinate of window position.
win_i <0~2>_width	0 ~ 320	0	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	0	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	0	4/4	Sensitivity of motion detection window.

Group: **ddns**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the dynamic dns.
provider	Safe100, DyndnsDynamic, DyndnsCustom, TZO, DHS, DynInterfree,	DyndnsDynamic	6/6	Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom) TZO => tzo.com

	CustomSafe100			DHS => dhs.org DynInterfree =>dyn-interfree.it CustomSafe100 => Custom server using safe100 method
<provider>_hostname	string[128]	<blank>	6/6	Your dynamic hostname.
<provider>_usernameemail	string[64]	<blank>	6/6	Your user or email to login ddns service provider
<provider>_passwordkey	string[64]	<blank>	6/6	Your password or key to login ddns service provider
<provider>_servername	string[128]	<blank>	6/6	The server name for safe100. (This field only exists for provider is customsafe100)

Group: upnppresentation

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	1	6/6	Enable or disable the UPNP presentation service.

Group: upnpportforwarding

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the UPNP port forwarding service.
upnpnatstatus	0~3	0	6/7	The status of UpnP port forwarding, used internally. 0 is OK, 1 is FAIL, 2 is no IGD router, 3 is no need to do port forwarding

Group: **syslog**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	0	6/6	enable remote log
serverip	<IP address>	<blank>	6/6	Log server IP address
serverport	514, 1025~65535	514	6/6	Server port used for log

level	0~7	6	6/6	The levels to distinguish the importance of information. 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

Group: **camctrl** (product dependent)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enablehttptunnel	<boolean>	0	4/4	Enable HTTP tunnel for camera control

Group: **camctrl_c<0~(n-1)>** for n channel product (capability.ptzenabled)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	0	1/4	Pan speed
tiltspeed	-5 ~ 5	0	1/4	Tilt speed
zoomspeed	-5 ~ 5	0	1/4	Zoom speed
autospeed	-5 ~ 5	0	1/4	Auto pan speed
focusspeed	-5 ~ 5	0	1/4	Auto focus speed
dwelling	0 ~ 9999	0	1/4	Time to dwelling when patrol
axisx	-104 ~ 104	0	1/7	Axis X coordinate, used internally
axisy	-15 ~ 28	0	1/7	Axis Y coordinate, used internally
preset_i<0~19>_name	string[40]	<blank>	1/4	The name of preset location
preset_i<0~19>_ dwelling	0 ~ 255	<blank>	1/4	The dwelling time of each preset location
uart	0 ~ (m-1), m is uart count	0	1/4	select correspond uart (capability.nuart>0)

cameraid	0~255	1	1/4	Camera ID to control external PTZ cameral
isptz	<boolean>	0	1/7	to distinguish the video channel if mapping to a PTZ camera
disablemdonptz	<boolean>	0	1/4	disable motion detection on PTZ operation
pantilt_port	<integer>	<blank>	1/4	The pan and tilt channel.
pantilt_camid	0 ~ 255	1	1/4	ID of camera on pan/tilt channel.
zoom_port	<integer>	<blank>	1/4	The zoom channel.
zoom_camid	0 ~ 255	1	1/4	ID of camera on zoom channel.

Group: **uart** (capability.nuart>0) (product dependent)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
ptzdrivers_i<0~19, 127>_name	string[40]	<blank>	1/4	The name of the PTZ driver
ptzdrivers_i<0~19, 127>_location	string[128]	<blank>	1/4	The full path of the PTZ driver
update	1	N/A	7/4	update the list of built-in external PTZ drivers
enablehttptunnel	<boolean>	0	4/4	Enable HTTP tunnel channel to control UART

Group:**uart_i<0~(n-1)>** n is uart port count (capability.nuart>0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
baudrate	110,300,600,1200,2400,3600,4800,7200,9600,19200,38400,57600,115200	9600	4/4	set baud rate of COM port
databit	5,6,7,8	8	4/4	data bits in a character frame
paritybit	none, odd,	none	4/4	For error checking

	even			
stopbit	1,2	1	4/4	1 2-1.5 , data bit is 5 2-2
uartmode	rs485, rs232	rs485	4/4	rs485 or rs232
uartreset	<boolean>	0	4/4	set this flag to true to apply change of UART configuration
customdrvcmd_i<0~9>	string[128]	NULL	1/4	PTZ command for custom camera.
speedlink_i<0~4>_name	string[40]	NULL	1/4	Additional PTZ command name
speedlink_i<0~4>_cmd	string[128]	NULL	1/4	Additional PTZ command list
ptzdriver	0~19, 127 (custom), 128 (no driver)	128 (no driver)	4/4	which PTZ driver is used by this COM port

Group: **privacymask_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable the privacy mask
win_i<0~4>_enable	<boolean>	0	4/4	Enable the privacy mask window
win_i<0~4>_name	string[14]	NULL	4/4	The name of privacy mask window
win_i<0~4>_left	0 ~ 320/352	0	4/4	Left coordinate of window position.
win_i<0~4>_top	0 ~ 240/288	0	4/4	Top coordinate of window position.
win_i<0~4>_width	0 ~ 320/352	0	4/4	Width of privacy mask window
win_i<0~4>_height	0 ~ 240/288	0	4/4	Height of privacy mask window

Group: capability

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	0200a	0100a	0/7	The HTTP API version.
bootuptime	<positive integer>	60	0/7	The server bootup time
nir	0, <positive integer>	0	0/7	number of IR interface
ndi	0, <positive integer>	1	0/7	number of digital input
ndo	0, <positive integer>	1	0/7	number of digital output
naudioin	0, <positive integer>	1	0/7	number of audio input
naudioout	0, <positive integer>	1	0/7	number of audio output
nvideoin	<positive integer>	1	0/7	number of video input
nmediastream	<positive integer>	2	0/7	number of media stream per channel
nvideosetting	<positive integer>	2	0/7	number of video settings per channel
naudiosetting	<positive integer>	1	0/7	number of audio settings per channel
nuart	0, <positive integer>	1	0/7	number of UART interface
ptzenabled	< positive integer >	2	0/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => Support camera control function 0(not support), 1(support) Bit 1 => Build-in or external camera.

				0(external), 1(build-in) Bit 2 => Support pan operation. 0(not support), 1(support) Bit 3 => Support tilt operation. 0(not support), 1(support) Bit 4 => Support zoom operation. 0(not support), 1(support) Bit 5 => Support focus operation. 0(not support), 1(support)
protocol_https	< boolean >	0	0/7	indicate whether to support http over SSL
protocol_rtsp	< boolean >	1	0/7	indicate whether to support rtsp
protocol_sip	<boolean>	1	0/7	indicate whether to support sip
protocol_maxconnection	<positive integer>	NULL	0/7	The maximum allowed simultaneous connections
protocol_rtp_multicast_scalable	<boolean>	1	0/7	indicate whether to support scalable multicast
protocol_rtp_multicast_backchannel	<boolean>	0	0/7	indicate whether to support backchannel multicast
protocol_rtp_tcp	<boolean>	1	0/7	indicate whether to support rtp over tcp
protocol_rtp_http	<boolean>	1	0/7	indicate whether to support rtp over http
protocol_spush_mjpeg	<boolean>	1	0/7	indicate whether to support server push motion jpeg
protocol_snmp	<boolean>	0	0/7	indicate whether to support snmp
videoin_type	0, 1, 2	1	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of the available resolution separates by comma)	176x144, 320x240, 640x480	0/7	available resolutions list

videoin_codec	<a list of the available codec types separaters by comma)	mpeg4, mjpeg	0/7	available codec list
videoout_codec	<a list of the available codec types separaters by comma)	NULL	0/7	available codec list
audio_aec	<boolean>	0	0/7	indicate whether to support acoustic echo cancellation
audio_extmic	<boolean>	1	0/7	indicate whether to support external microphone input
audio_linein	<boolean>	1	0/7	indicate whether to support external line input
audio_lineout	<boolean>	1	0/7	indicate whether to support line output
audio_headphoneout	<boolean>	0	0/7	indicate whether to support headphone output
audioin_codec	<a list of the available codec types separaters by comma)	aac4, gamr	0/7	available codec list
audioout_codec	<a list of the available codec types separaters by comma)	NULL	0/7	available codec list
uart_httptunnel	<boolean>	0	0/7	Indicate whether to support the http tunnel for uart transfer
transmission_mode	Tx, Rx, Both	Tx	0/7	Indicate what kind of transmission mode the machine used. TX: server, Rx: receiver box, Both: DVR?.
network_wire	<boolean>	1	0/7	Indicate whether to support the Ethernet

network_wireless	<boolean>	0	0/7	Indicate whether to support the wireless
wireless_802dot11b	<boolean>	0	0/7	Indicate whether to support the wireless 802.11b+
wireless_802dot11g	<boolean>	0	0/7	Indicate whether to support the wireless 802.11g
wireless_encrypt_wep	<boolean>	0	0/7	Indicate whether to support the wireless WEP
wireless_encrypt_wpa	<boolean>	0	0/7	Indicate whether to support the wireless WPA
wireless_encrypt_wpa2	<boolean>	0	0/7	Indicate whether to support the wireless WPA2
derivative_brand	<boolean>	1	0/7	Indicate whether to support upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
iva	<boolean>	1	0/7	Indicate whether to support the Intelligent Video Analysis

Group: event_i<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	The identification of this entry
enable	0, 1	0	6/6	To enable or disable this event.
priority	0, 1, 2	1	6/6	Indicate the priority of this event. "0" indicates low priority. "1" indicates normal priority. "2" indicates high priority.
delay	1~999	10	6/6	Delay seconds before detect next event.

trigger	boot, di, motion, seq, iva	boot	6/6	Indicate the trigger condition. "boot" indicates system boot. "di" indicates digital input. "motion" indicates video motion detection. "seq" indicates periodic condition. "iva" indicates Intelligent Video Analysis.
di	<integer>	0	6/6	Indicate which di detected. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.
mdwin	<integer>	0	6/6	Indicate which motion detection windows detected. This field is required when trigger condition is "md". One bit represents one window. The LSB indicates the 1^{st} window. For example, to detect the 1^{st} and 3^{rd} windows, set mdwin as 5.
inter	1~999	1	6/6	Interval of period snapshot in minute. This field is used when trigger condition is "seq".

weekday	<interger>	127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. The bit0 (LSB) indicates Saturday. The bit1 indicates Friday. The bit2 indicates Thursday. The bit3 indicates Wednesday. The bit4 indicates Tuesday. The bit5 indicates Monday. The bit6 indicates Sunday. For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	00:00	6/6	Begin time of weekly schedule.
endtime	hh:mm	24:00	6/6	End time of weekly schedule. (00:00 ~ 24:00 means always.)
action_do_i<0~(ndo-1)>_enable	0, 1	0	6/6	To enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	1	6/6	The duration of digital output is triggered in seconds.
action_server_i<0~4>_enable	0, 1	0	6/6	To enable or disable this server action. The default value is 0.
action_server_i<0~4>_media	NULL, 0~4	NULL	6/6	The index of attached media.

Group: server_i<0~4>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	The identification of this entry
type	email, ftp, http, ns	email	6/6	Indicate the server type. “email” is email server. “ftp” is ftp server. “http” is http server. “ns” is network storage.
http_url	string[128]	http://	6/6	The url of http server to upload.

http_username	string[64]	NULL	6/6	The username to login in the server.
http_passwd	string[64]	NULL	6/6	The password of the user.
ftp_address	string[128]	NULL	6/6	The ftp server address
ftp_username	string[64]	NULL	6/6	The username to login in the server.
ftp_passwd	string[64]	NULL	6/6	The password of the user.
ftp_port	0~65535	21	6/6	The port to connect the server.
ftp_location	string[128]	NULL	6/6	The location to upload or store the media.
ftp_passive	0, 1	1	6/6	To enable or disable the passive mode. 0 is to disable the passive mode. 1 is to enable the passive mode.
email_address	string[128]	NULL	6/6	The email server address
email_username	string[64]	NULL	6/6	The username to login in the server.
email_passwd	string[64]	NULL	6/6	The password of the user.
email_senderemail	string[128]	NULL	6/6	The email address of sender.
email_recipientemail	string[128]	NULL	6/6	The email address of recipient.
ns_location	string[128]	NULL	6/6	The location to upload or store the media.
ns_username	string[64]	NULL	6/6	The username to login in the server.
ns_passwd	string[64]	NULL	6/6	The password of the user.
ns_workgroup	string[64]	NULL	6/6	The workgroup for network storage.

Group: media_i<0~4>(media_freespace is used internally.)

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	The identification of this entry
type	snapshot, systemlog videoclip	snapshot	6/6	The media type to send to the server or store by the server.

snapshot_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
snapshot_prefix	string[16]	NULL	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	0	6/6	To add date and time suffix to filename or not. 1 means to add date and time suffix. 0 means not to add it.
snapshot_preevent	0 ~ 7	1	6/6	It indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	1	6/6	The number of post-event images.
videoclip_source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
videoclip_prefix	string[16]	NULL	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	0	6/6	It indicates the time of pre-event recording in seconds.
videoclip_maxduration	1 ~ 10	5	6/6	The time of maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 1500	500	6/6	The maximum size of one video clip file in Kbytes.

Group: recording_i<0~1>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	The identification of this entry
enable	0, 1	0	6/6	To enable or disable this recoding.

priority	0, 1, 2	1	6/6	Indicate the priority of this recoding. “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.
source	<integer>	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
weekday	<interger>	127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. The bit0 (LSB) indicates Saturday. The bit1 indicates Friday. The bit2 indicates Thursday. The bit3 indicates Wednesday. The bit4 indicates Tuesday. The bit5 indicates Monday. The bit6 indicates Sunday. For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	00:00	6/6	Begin time of weekly schedule.
endtime	hh:mm	24:00	6/6	End time of weekly schedule. (00:00~24:00 means always.)
prefix	string[16]	NULL	6/6	Indicate the prefix of the filename.
cyclesize	<integer>	500	6/6	The maximum size for cycle recording in Kbytes.
maxfilesize	50~6000	50	6/6	The max size for one file in Kbytes
dest	0~4	0	6/6	The destination to store the recording data. “cf” means CF card. “0~4” means the index of network storage.

Group: iva_i<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	Trigger<1~3>	4/4	The identification of this entry.
enable	0, 1	0	4/4	To enable or disable this Video content analysis.
type	move, loiter, obstruct	Obstruct	4/4	The type of the trigger.
Delay	1~999	10	4/4	How many seconds when the object(s) loiter in the region should the event be triggered.
region_i<0~4>_name	string[40]	NULL	4/4	The name of the region.
region_i<0~4>_points	string[40]	NULL	4/4	The coordinates of the points. For example. 72,(the x of point 1) 90,(the y of point 1) 202, (the x of point 2) 42,...

Drive the digital output

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/setdo.cgi?do1=<*state*>[&do2=<state>]
[&do3=<state>][&do4=<state>][&return=<*return page*>]

Where state is 0, 1. "0" means inactive or normal state while "1" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – inactive, normal state
		1 – active, triggered state
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page.

Example: Drive the digital output 0 to triggered state and redirect to an empty page

http://myserver/cgi-bin/dido/setdo.cgi?do0=1

Query status of the digital input

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]

If no parameter is specified, all the status of digital input will be returned.

Return:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: <*length*>\r\n

\r\n

[di0=<*state*>]\r\n

[di1=<*state*>]\r\n

[di2=<*state*>]\r\n

[di3=<*state*>]\r\n

where <*state*> can be 0 or 1.

Example: Query the status of digital input 0

Request:

http://myserver/cgi-bin/dido/getdi.cgi?di0

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

\r\n

di0=1\r\n

Query status of the digital output

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]
```

If no parameter is specified, all the status of digital output will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[do0=<state>]\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
[do3=<state>]\r\n
```

where *<state>* can be 0 or 1.

Example: Query the status of digital output 0

```
Request:
http://myserver/cgi-bin/dido/getdo.cgi?do0

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
do0=1\r\n
```

Capture single snapshot

Note: This request require normal user privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>]
```

If the user requests the size larger than all stream setting on the server, this request will failed!

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	the channel number of video source
resolution	<available resolution>	0	The resolution of image
quality	1~5	3	The quality of image

Server will return the most up-to-date snapshot of selected channel and stream in JPEG format. The size and quality of image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

Account management

Note: This request requires administrator privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<name>[&userpass=<value>][&privilege=<value>]
[&privilege=<value>][...][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
method	add	Add an account to server. When using this method, “username” field is necessary. It will use default value of other fields if not specified.

	delete	Remove an account from server. When using this method, “username” field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, “username” field is necessary, and other fields are optional. If not specified, it will keep original settings.
username	<name>	The name of user to add, delete or edit
userpass	<value>	The password of new user to add or that of old user to modify. The default value is an empty string.
privilege	<value>	The privilege of user to add or to modify.
	viewer	viewer’s privilege
	operator	operator’s privilege
	admin	administrator’s privilege
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page.

System logs

Note: This request require administrator privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/syslog.cgi
```

Server will return the up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

Upgrade firmware

Note: This request requires administrator privilege

Method: POST

Syntax:

http://<*servername*>/cgi-bin/admin/upgrade.cgi

Post data:

fimage=<file name>[&return=<return page>]\r\n

\r\n

<multipart encoded form data>

Server will accept the upload file named <file name> to be upgraded the firmware and return with <return page> if indicated.

Camera Control (capability.ptzenabled=1)

Note: This request requires privilege of viewer

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/camctrl.cgi?[channel=<value>][&camid=<value>][&move=<value>][&focus=<value>][&iris=<value>][&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>][&auto=<value>][&zoom=<value>][&speedlink=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source
camid	0,<positive integer>	Camera ID
move	home	Move to camera to home position
	up	Move camera up
	down	Move camera down
	left	Move camera left

	right	Move camera right
speedpan	-5 ~ 5	Set the pan speed
speedtilt	-5 ~ 5	Set the tilt speed
speedzoom	-5 ~ 5	Set the zoom speed
speedapp	-5 ~ 5	Set the auto pan/patrol speed
auto	pan	Auto pan
	patrol	Auto patrol
	stop	Stop camera
zoom	wide	To zoom for larger view with current speed
	tele	To zoom for farer view with current speed
focus	auto	To do auto focus
	far	To focus on farer distance
	near	To focus on nearer distance
speedlink	0 ~ 4	Issue speed link command.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Recall (capability.ptzenabled=1)

Note: This request requires privilege of viewer

Method: GET

Syntax:

http://<*servername*>/cgi-bin/viewer/recall.cgi?
recall=<value>[&channel=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
recall	Text string less than 30 characters	One of the present positions to recall.

channel	<0~(n-1)>	channel of video source
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

System Information

Note: This request requires normal user privilege (obsolete)

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/sysinfo.cgi

Server will return the system information. In HTTP API version 2, the CapVersion will be 0200. All the fields in the previous version (0100) is obsolete. Please use "getparam.cgi?capability" instead.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
Model=<model name of server>\r\n
CapVersion=0200\r\n
```

PARAMETER(supported capability version)	VALUE	DESCRIPTION
Model	system.firmwareversion	Model name of server. Ex:IP3133-VVTK-0100a
CapVersion	MMmm, MM is major version from 00 ~ 99 mm is minor version from 00 ~ 99 ex: 0100	The capability field version

Preset Locations (capability.ptzenabled=1)

Note: This request requires operator privilege

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/preset.cgi?[channel=<value>] [&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
addpos	<Text string less than 30 characters>	Add one preset location to preset list.
channel	<0~(n-1)>	channel of video source
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

IP filtering

Note: This request requires administrator access privilege

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/ipfilter.cgi? method=<value>&[start=<*ipaddress*>&end=<*ipaddress*>][&index=<*value*>] [&return=<return page>]

PARAMETER	VALUE	DESCRIPTION

Method	addallow	Add a set of allow IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
	adddeny	Add a set of deny IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
	deleteallow	Remove a set of allow IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove a set of deny IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The start IP address to add or to delete.
end	<ip address>	The end IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according the the current path. If you omit this parameter, it will redirect to an empty page.

UART HTTP tunnel channel (capability.nuart>0)

Note: This request requires operator privilege

Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/operator/uartchannel.cgi?[channel=<value>]
------------------------------------------------------------------------
GET /cgi-bin/operator/uartchannel.cgi?[channel=<value>]
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
```

```
cache-control: no-cache


-----------------------------------------------------------------------
POST /cgi-bin/operator/uartchannel.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in the GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through some proxy server.

This channel will help to transfer the raw data of UART over network.

PARAMETER	VALUE	DESCRIPTION
channel	0 ~ (n-1)	The channel number of UART.

Get SDP of Streamings

Note: This request requires viewer access privilege

Method: GET/POST

Syntax:

```
http://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

“m” is the stream number.

“network_accessname_<0~(m-1)>” is the accessname for stream “1” to stream “m”. Please refer to the “subgroup of network: rtsp” for setting the accessname of SDP.

You can get the SDP by HTTP GET method.

Open the network streamings

Note: This request requires viewer access privilege

Syntax:

For http push server (mjpeg):

http://<*servername*>/<network_http_s<0~m-1>_accessname>

For rtsp (mp4), user needs to input the url below for a rtsp compatible player.

rtsp://<*servername*>/<network_rtsp_s<0~m-1>_accessname>

“m” is the stream number.

For detailed streaming protocol, please refer to “control signaling” and “data format” documents.

Technical Specifications

Specifications

System
· CPU: VVTK-1000 SoC
· Flash: 8MB
· RAM: 64MB
· DSP:TI DM642
· Embedded OS: Linux 2.4

Lens
· CS-mount, vari-focal, f=2.9 mm ~ 8.2 mm, auto-iris
· IR Corrected
· Removable IR-cut filter for day & night function

Angle of view
· 26.7° ~ 69.0° (horizontal)
· 20.0° ~ 51.0° (vertical)

Shutter Time
· 1/30 sec. to 1/15000 sec.

Image Sensor
· SONY 1/4" Progressive scan CCD sensor in VGA resolution

Minimum Illumination
· 1.0 Lux/F1.0

Video Content Analysis
· Camera tampering detection
· Intelligent moving object detection
· Moving object loitering detection

Video
· Compression: MJPEG & MPEG-4
· Streaming:
Simultaneous dual-streaming
MPEG-4 streaming over UDP, TCP, or HTTP
MPEG-4 multicast streaming
MJPEG streaming over HTTP
· Supports 3GPP mobile surveillance
· Frame rates: 640x480 up to 30fps (60 Hz)/25fps (50Hz)

Image settings
· Adjustable image size, quality, and bit rate
· Time stamp and text caption overlay
· Flip & mirror
· Configurable brightness, contrast, and saturation
· AGC, AWB, AES
· Automatic or manual day/night mode
· Backlight compensation (BLC)
· Supports privacy masks

Audio
· Compression:
GSM-AMR speech encoding, bit rate: 4.75 kbps to 12.2 kbps
MPEG-4 AAC audio encoding, bit rate: 16 kbps to 128 kbps
· Interface:
Built-in microphone
External microphone input
Audio output
· Supports two-way audio by SIP protocol
· Supports audio mute

Networking
· 10/100 Mbps Ethernet, RJ-45
· Protocols: IPv4, TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, and PPPoE

Alarm and Event Management
· Triple-window video for motion detection
· One D/I and one D/O for external sensor and alarm
· Event notification using HTTP, SMTP, or FTP
· Local recording of MP4 files

Security
· Multi-level user access with password protection
· IP address filtering

Users
· Camera live viewing for up to 10 clients

Dimension (including lens)
· 205.5 mm (D) x 82.1 mm (W) x 51.2 mm (H)

Weight (including lens)
· Net: 545 g

LED Indicator
· System power and status indicator
· System activity and network link indicator

Power
· 12V DC, 24V AC
· Consumption: Max 7.5 W
· 802.3af compliant Power over Ethernet

Approvals
· CE, FCC, C-Tick, LVD, VCCI

Operating Environments
· Temperature: 0° ~ 50° C (32° ~ 122° F)
· Humidity: 20 % ~ 80 % RH

Viewing System Requirements
· OS: Microsoft Windows 2000/XP/Vista
· Browser: Internet Explorer 6.x or above
· Cell phone: 3GPP player
· Real Player: 10.5 or above
· Quick Time: 6.5 or above

Installation, Management , and Maintenance
· Installation Wizard 2
· 16-CH recording software
· Supports firmware upgrade

Applications
· SDK available for application development and system integration

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT REGARD TO PC SOFTWARE, YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

USA - This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

Europe CE – This digital equipment fulfills the requirement for radiated emission according to limit B of EN55022/1998, and the requirement for immunity according to EN50082-1/1992.

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.